



TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

SANNA-MARIA HIRVONEN
LIIKKUVAN TYÖKONEEN TURVALLISUUS
Diplomityö

Tarkastaja: prof. Kalevi Huhtala
Tarkastaja ja aihe hyväksytty
Teknisten tieteiden tiedekuntaneu-
voston kokouksessa 9. Huhtikuuta
2014

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO

Automaation koulutusohjelma

HIRVONEN, SANNA-MARIA: Liikkuvan työkoneen turvallisuus

Diplomityö, 81 sivua, 2 liitesivua

Elokuu 2014

Pääaine: Koneautomaatio

Tarkastaja: professori Kalevi Huhtala

Avainsanat: Liikkuva työkone, koneasetus, koneturvallisuus, koneturvallisuus standardit, hydraulijärjestelmän luotettavuus, toiminnallinen turvallisuus, riskianalyysi, riskien pienentäminen, suoritustaso, todentaminen ja kelpuutus, reaaliaikainen simulointi.

Liikkuvan työkoneen turvallisuus on osa laadukasta koneenrakennustyötä. Koneturvallisuuden määrittelee konedirektiivi sekä valtioneuvoston asetus koneiden turvallisuudesta. Liikkuvan työkoneen turvallisuus osoitetaan vaatimustenmukaisuusvakuutuksella, joka koneen valmistajan on allekirjoitettava. Liikkuva työkone täyttää konedirektiivin ja koneasetuksen turvallisuusvaatimukset, jos se on valmistettu yhdenmukaistettujen standardien ohjeistuksien mukaan.

Standardit ohjeistavat liikkuvan työkoneen eri osajärjestelmien suunnittelua. Tässä diplomityössä käsitellään hydraulijärjestelmää ja ohjausjärjestelmää. Koneasetuksen vaatimuksen mukaan koneen valmistajan on tehtävä riskinarviointi, ja suunniteltava kone arvioinnin tulokset huomioon ottaen.

Tämän diplomityön lähtökohta on käydä läpi liikkuvan työkoneen koko elinkaareen liittyvät turvallisuusvaatimukset ja suunnittelun prosessit. Liikkuvan työkoneen turvallisuutta tarkastellaan hydraulijärjestelmän luotettavuuden ja ohjausjärjestelmän toiminnallisen turvallisuuden kautta. Koneasetuksen vaatimukset ja standardien ohjeistukset ovat koko prosessin pohjana.

Turvallisuusvaatimusten täyttyminen, ja toiminnallisen turvallisuuden ylttäminen vaaditulle tasolle, varmistetaan todentamisella ja kelpuutuksella. Liikkuva työkone on monimutkainen järjestelmä, jossa yhden virheen vaikutusta koko järjestelmään on vaikeaa analysoida kattavasti. Reaaliaikainen simulointi on luotettava, ja vaatimustenmukainen tapa turvallisuusvaatimusten testaukseen ja todentamiseen.

Liikkuvan työkoneen täyttämät turvallisuusvaatimukset on dokumentoitava. Näistä dokumenteista koostetaan vaatimustenmukaisuusvakuutus. Kun suunnitteluvaiheessa tiedetään, mitä dokumentteja tarvitaan työkoneen turvallisuuden osoittamiseksi, tulee asiakirjojen luominen ja liikkuvan työkoneen turvallisuusvaatimukset luontaiseksi osaksi koneenrakennusta.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY

Master's Degree Programme in Automation Technology

HIRVONEN, SANNA-MARIA: Safety of mobile work machine

Master of Science Thesis, 81 pages, 2 Appendix pages

August 2014

Major: Machinery automation

Examiner: Professor Kalevi Huhtala

Keywords: Mobile work machine, Safety of machinery, machinery directive, standards, reliability of hydraulics, risk assessment, risk reduction, safety level, verification and validation, real time simulation.

Safety of machinery is an important part of machine construction. General safety requirements are prescribed in the directive on machinery as well as in the Government decree on safety of machinery. Machinery manufacturers sign the Declaration of Conformity, which assures that the mobile work machine meets the requirements of the given directive. When the machinery manufactures are devoted to follow the machinery safety standards, the machines will also meet the appropriate safety requirements.

Safety standards contain detailed technical requirements for machines and their subsystems. This Master's Thesis is about mobile work machines' hydraulic and control systems. Machinery manufacturers are responsible for carrying out systems risk assessment according to in Finland Government decree on safety of machinery.

This Master's thesis presents the safety requirements which are assigned to mobile work machines for their life cycle. Safety of machinery is based on reliability of hydraulic systems. Functional safety, again, is a key to control systems risk reduction. All phases are based on standards of machinery safety.

The phases of verification and validation assure that machine meets its respective safety requirements. Hydraulic mobile machines are complex systems and one error can have many consequences. Some effects may not be easily recognizable and may cause hazard. Real time simulation helps to identify these effects.

It is manufacturer's responsibility to ensure that all phases are documented. The manufacturer can use the technical file, where necessary, to attest the machine's conformity to the respective regulations.

ALKUSANAT

Kokemus koneenrakennuksesta osoittaa, että liikkuvien työkoneiden turvallisuussuunnittelu on varsinkin pienissä ja keskisuurissa yrityksissä, vielä lähtökuopissa. Työkoneen turvallisuutta pidetään tärkeänä, mutta lakien ja asetusten sisällön heikko tunteminen saa turvallisuussuunnittelun tuntumaan hankalalta ja aikaa vievältä. Koneturvallisuuden asetukset ja standardit ovat helpommin sovellettavissa prosessiautomaation koneille kuin liikkuville työkoneille. Tämä diplomityö sai alkunsa tarpeesta saada yhteenveto koneturvallisuuteen liittyvien asetusten ja standardien hyödyntämisestä älykkäiden liikkuvien työkoneiden suunnittelussa.

Haluan kiittää Tampereen teknillisen yliopiston, hydrauliiikan- ja automatiikan laitoksen johtajaa ja diplomityön tarkastajaa professori Kalevi Huhtalaa siitä, että hän mahdollisti tämän diplomityön teon. Erityisesti haluan kiittää tutkija Miika Ahopeltoa avusta työn suunnittelussa ja ohjauksesta simulointimallin kanssa. Lämpimät kiitokset myös diplomi-insinööri Elina Hihnala-Mäkelälle, jonka ohjauksella sain diplomityön päätökseen, sekä oikeinkirjoituksen tarkastajalle Katja Palanteelle. Haluan muistaa kaikkia hydrauliiikan- ja automatiikan laitoksen työntekijöitä, jotka vuosien varrella ovat jaksaneet muistuttaa minua valmistumisesta, nyt se on totta. Ja kiitokset Markolle, kun kuitenkin yritit ymmärtää.

Erityiskiitokset vanhemmilleni Pirjolle ja Raimolle, jotka useasti ajoivat pitkän matkan päästääkseen minut rauhassa kirjoittamaan diplomityötä. Ilman teidän apua ei diplomityö olisi valmistunut määräajassa.

Tampereella 22.7.2014

Sanna-Maria Hirvonen

SISÄLLYS

Tiivistelmä.....	ii
Abstract	iii
Alkusanat.....	iv
Lyhenteet ja termit	vi
1 Johdanto.....	1
2 Liikkuvan työkoneen hydraulijärjestelmä	3
2.1 Ohjausjärjestelmä	4
2.2 Ajovoimansiirto.....	6
2.3 Työhydrauliikka	8
2.4 Hydraulijärjestelmän luotettavuus.....	9
2.4.1 Venttiilit	12
2.4.2 Hydraulipumput ja toimilaitteet	14
2.4.3 Letkut ja putket.....	15
2.4.4 Suodattimet	16
3 Koneiden turvallisuutta koskevat säädökset.....	18
3.1 Standardit	19
3.2 Yleiset suunnitteluperiaatteet	21
3.2.1 Koneen raja-arvot	22
3.2.2 Vaarojen tunnistaminen	23
3.2.3 Riskin suuruuden arviointi	25
3.2.4 Riskin merkityksen arviointi	26
3.2.5 Riskin pienentäminen	26
3.3 Turvallisuuteen liittyvät ohjausjärjestelmän osat.....	27
3.3.1 Suoritustaso ja turvallisuuden eheyden taso	32
3.4 Toiminnallinen turvallisuus	36
3.5 Hydraulinen tehonsiirto	39
4 Liikkuvan työkoneen turvallisuussuunnittelu	41
4.1 Riskianalyysi	45
4.2 Riskien pienentäminen	51
4.3 Todentaminen ja kelpuutus	56
4.3.1 Hydrauliikka.....	56
4.3.2 Ohjelmistot.....	58
5 CASE: Turvatoiminnon suunnittelu puomin vikaantumiseen.....	60
5.1 Turvatoiminnon määrittelemineen	61
5.2 Turvatoiminnon suunnittelu ja toteuttaminen.....	65
5.3 Turvatoiminnon arviointi.....	71
6 Tulokset	73
7 Yhteenveto	75
Lähteet.....	78
Liitteet	82

LYHENTEET JA TERMIT

λ	Vikataajuus
λ_D	Vaarallisen vikaantumisen taajuus
λ_S	Turvallisen vikaantumisen taajuus
β	Yhteisvikaantumisalttius
ε_m	Moottorin kulman asetus
ε_p	Pumpun kulman asetus
η_{mhm}	Moottorin mekaanishydraulinen hyötysuhde
η_{mhp}	Pumpun mekaanishydraulinen hyötysuhde
η_{vm}	Moottorin volumetrinen hyötysuhde
η_{vp}	Pumpun volumetrinen hyötysuhde
DC	Diagnostiikan kattavuus
M_m	Moottorin antama momentti
M_p	Pumpun ottama momentti
MTTF _d	Vaarallinen keskimääräinen vikaantumisaika
n_m	Moottorin kierrosnopeus
n_p	Pumpun kierrosnopeus
PFH _d	Vaarallisen vikaantumisen todennäköisyyden kynnsarvo
PL	Suoritustaso
S/E/OE	Sähköinen, elektroninen ja ohjelmoitava elektroninen
SIL	Eheystaso
T1	Määräaikaistarkastuksen aikaväli tai elinkaaren pituus
T2	Diagnostiikkatestauksen aikaväli
V_m	Moottorin kierrostilavuus
V_p	Pumpun kierrostilavuus

1 JOHDANTO

Koneiden turvallisuutta koskee valtioneuvoston asetus koneiden turvallisuudesta (400/2008). Koneasetuksella pannaan täytäntöön konedirektiivi (2006/42/EY). Koneasetus on koneenrakentajia velvoittava asetus, sen noudattaminen on laissa määrätty. Koneasetus koskee koneita, vaihdettavia laitteita, turvakomponentteja, nostoapuvälineitä, nostoketjuja, -vöitä, -köysiä, nivelakseleita ja osittain valmiita koneita.

Koneilla tarkoitetaan toisiinsa liitettyjen osien tai komponenttien yhdistelmää, jota käytetään muulla kuin eläin- tai ihmisvoimalla, ja jossa ainakin yksi osa tai komponentti on liikkuva ja joka on kokoonpantu erityistä toimintoa varten. Koneasetuksen liitteessä I on erikseen huomioitu päältä ajettavat omalla käyttövoimalla liikkuvat koneet. Muutoin liikkuvien työkoneiden kannalta lakia, asetuksia ja standardeja joudutaan soveltamaan, sillä selkeää yhteenvetoa liikkuvien työkoneiden turvallisuudesta ei ole.

Liikkuvien työkoneiden mekaanisille rakenteille ja hydrauliselle tehonsiirrolle on omat säädöksensä. Päältä ajettavien työkoneiden ohjaamoille on omat ergonomiasäädöksensä, lisäksi melua ja tärinää tulee mitata ja rajoittaa hyväksyttävään tasoon. Nykyaikaisissa liikkuvissa työkoneissa on yhä enemmän sähkö-, elektroniikka- ja ohjelmoitavia elektroniikkajärjestelmiä, jotka ovat keskeisessä asemassa koneturvallisuuden toteutuksessa. Ohjelmoitavat järjestelmät mahdollistavat toiminnallisen turvallisuuden hyödyntämisen, mutta järjestelmä on todennettava ja kelpuutettavaa. Liikkuvan työkoneen turvalliseksi saattaminen on monen eri osa-alueen hallintaa ja ymmärtämistä.

Tässä diplomityössä tutkitaan liikkuvan työkoneen turvallisuuden ominaisia piirteitä ja huomioon otettavia asioita. Diplomityö on rajattu koskemaan liikkuvan työkoneen hydraulikkaa, ohjausjärjestelmää ja toiminnallista turvallisuutta, sekä työkoneen riskienhallintaa. Liikkuvat työkoneet eivät ole enää mekaanis-hydraulisia järjestelmiä, vaan ohjelmoitavia sähköisiä järjestelmiä. Sähköisten-, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien turvallisuus on osa liikkuvan työkoneen turvalliseksi tekemistä. Tässä diplomityössä liikkuvalla työkoneella tarkoitetaan älykkäitä liikkuvia työkoneita.

Liikkuvan työkoneen turvallisuus pohjautuu standardeihin ja niiden viemiseen osaksi koneensuunnittelua. Diplomityön luvussa kaksi määritellään liikkuvan työkoneen hydraulijärjestelmä, jonka muodostavat ohjausjärjestelmä, ajovoimansiirto ja työhydraulikka. Eri järjestelmät esitetään pintapuolisesti toiminnan ja komponenttien näkökulmasta.

Lopuksi tarkastellaan hydraulikan luotettavuutta koneturvallisuuden kannalta. Luvussa kolme avataan tärkeimpien standardien sisältö: Yleiset suunnitteluperiaatteet SFS-EN ISO 12100, ohjausjärjestelmä SFS-EN ISO 13849, toiminnallinen turvallisuus SFS-EN 61508 ja hydraulinen tehonsiirto SFS-EN ISO 4413. Luvussa neljä käydään samat standardit läpi liikkuvien työkoneiden ja niiden suunnittelun näkökulmasta. Luvussa viisi viedään teoria lähemmäksi käytäntöä. Edellä esiteltyt standardit hyödynnetään suunniteltaessa turvatoimintoa Tampereen teknillisen yliopiston hydraulikan ja automatiikan laitoksella tutkimuskäytössä olevalle GIM-koneelle. Teleskooppipuomin hydraulijärjestelmään turvatoiminto toteutetaan ja testataan GIMsim simulointijärjestelmällä. GIM-kone ja simulointijärjestelmä ovat osa hydraulikan ja automatiikan laitoksen The Generic Intelligent Machine projektia. Turvatoimintoa suunniteltaessa ja toteutettaessa tutkitaan niin pienkuormaajien tapaturmatilastoihin, kun pohditaan simuloinnin tuomia etuja koneturvallisuuteen.

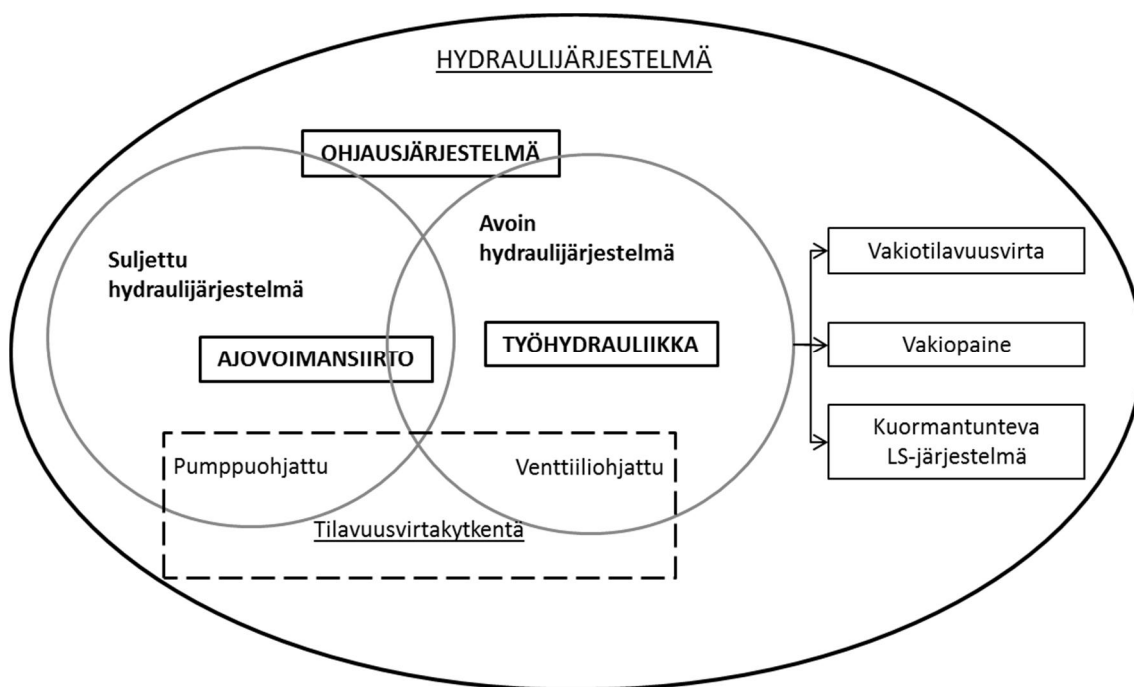
Diplomityö ei ole kaiken kattava ohjekirja liikkuvan työkoneen turvallisuutta suunniteltaessa. Työ kannustaa ottamaan turvallisuusnäkökulman osaksi koneensuunnittelua ja osoittaa ne kohdat, jotka suunnittelussa tulisi turvallisuuden kannalta huomioida. Niin kauan kuin koneturvallisuus mielletään vaikeaksi tulkita, se katsotaan myös hankalaksi toteuttaa. Liikkuvissa työkoneissa hyväksytään suurempia jäännösriskejä kuin prosessi-automaation koneissa, työkoneiden työskentelytapojen ja ominaisuuksien vuoksi. Älykkäissä liikkuvissa työkoneissa voidaan käyttää toiminnallisen turvallisuuden keinoja riskien pienentämiseksi. Reaaliaikaiset simulointijärjestelmät mahdollistavat ohjelmallisesti tehtyjen turvatoimintojen suunnittelun, toteutuksen ja testauksen. Reaaliaikaista simulointijärjestelmää voidaan hyödyntää jo riskianalyysia tehtäessä. Simuloinnin avulla pystytään tutkimaan yhden vian vaikutusta koko järjestelmään. Simulointijärjestelmässä tehtävät muutokset ja niiden testaukset eivät aiheuta merkittäviä kustannuksia ja työkoneen käyttöönottovaihe nopeutuu. Reaaliaikaisella simuloinnilla voidaan varmistaa niiden menetelmien toimivuus, joilla riskejä on poistettu tai pienennetty.

2 LIKKUVAN TYÖKONEEN HYDRAULIJÄRJESTELMÄ

Liikkuvalla työkoneella tarkoitetaan moottorikäyttöistä, pyörillä tai telaketjuilla liikkuvaa konetta, jota ohjataan koneen ohjaamosta käsin tai kauko-ohjauksella koneen ulkopuolelta. Liikkuvassa työkoneessa on lisäksi erilaisia toimilaitteita, jotka muodostavat liikkuvan työkoneen työlaitteet. Käyttömoottori, yleensä dieselmoottori, on koneen ydin ja se tuottaa tehoa muun muassa hydraulijärjestelmälle. Hydraulijärjestelmän tehtävä on tuottaa hydraulienergiaa ja siirtää se toimilaitteille, joiden avulla tuotetaan voimaa ja liikettä. Hydraulienergiaa tuottavan osan ja sitä käyttävien toimilaitteiden lisäksi järjestelmässä on hydraulienergiaa ja sen suuntaa säättäviä komponentteja. Komponentteja ja toimilaitteita yhdistää putkisto ja letkusto, joissa liikkuvan väliaineen kautta hydraulienergiaa siirretään.

Liikkuva työkone voidaan jakaa kolmeen hydraulijärjestelmään: ohjausjärjestelmään, ajovoimansiirtoon ja työhydrauliikkaan. Ohjausjärjestelmä vastaa toimilaitteiden ja ajovoimansiirron ohjauksesta ja hallinnasta. Ohjausjärjestelmä sisältää myös ohjauskäskyt toimilaitteiden välillä. Ohjauskäskyt voivat olla mekaanisia, hydraulisia tai sähköisiä. Ajovoimansiirron ja työhydrauliikan tehtävänä on muuntaa mekaaninen energia hydrauliseksi energiaksi pumppujen avulla, sekä siirtää se putkien ja letkujen kautta toimilaitteille. [1.]

Hydraulijärjestelmät voidaan edelleen jakaa tilavuusvirtakytkentäiseen ja painekytken-
täiseen järjestelmään. Liikkuvissa työkoneissa käytetään tilavuusvirtakytkentäistä järjestelmää, jossa toimilaitteelle tuleva tilavuusvirta määräytyy hydraulipumpuissa ja toimilaitteen kuorman suuruus määrää järjestelmän painetason. Tilavuusvirtakytkentäinen järjestelmä voi olla joko suljettu tai avoin piiri. [1.] Avoin hydraulijärjestelmä on venttiiliohjattu piiri, jota käytetään tavallisesti työhydrauliikassa, kun taas ajovoimansiirto on pumppuohjattu suljettu piiri. Kuvassa 1 on esitetty periaatteellinen hydraulijärjestelmien jakotapa.



Kuva 1 Hydraulijärjestelmä voidaan jakaa moneen eri osaan

Liikkuvan työkonteen tulee noudattaa valtioneuvoston asetusta koneiden turvallisuudesta (400/2008), niin sanottua koneasetusta, joka pohjautuu Euroopan parlamentin ja neuvoston konedirektiiviin (2006/42/EY).

2.1 Ohjausjärjestelmä

Ohjausjärjestelmä määritellään standardin SFS-EN 62601 [2] mukaan järjestelmäksi, joka reagoi muista koneen osista, käyttäjältä tai ulkoisista ohjauslaitteista tuleviin tietoihin, ja joka saa aikaan lähtötiedot, joiden avulla kone saadaan liikkumaan tarkoituksenmukaisesti. Kun puhutaan ohjausjärjestelmästä liikkuvan työkonteen hydraulijärjestelmän osana, tarkoittaa ohjausjärjestelmä niitä hydraulisia ja sähköhydraulisia komponentteja, joilla tarkoituksenmukainen käyttäytyminen saadaan aikaan. Liikkuvat työkonet ovat enemmän ohjelmoitavia järjestelmiä kuin mekaanishydraulisia koneita, joten nämä kaksi ohjausjärjestelmän määritelmää sekoittuvat toisiinsa. Tässä luvussa ohjausjärjestelmästä puhutaan hydraulisten komponenttien tasolla ja myöhemmin koneturvallisuuden yhteydessä ohjausjärjestelmä nähdään tietokonepohjaisena ohjelmoitavana järjestelmänä sähköisine toimilaitteineen.

Ohjausjärjestelmä vastaa liikkuvan työkonteen ohjausliikkeistä niin ajovoimansiirrossa kuin työhydraulikan toimilaitteillakin. Ohjausjärjestelmä voi olla hydraulinen, mekaanishydraulinen, sähköhydraulinen tai sähköinen. Hydraulisessa ja mekaanishydraulisessa ohjausjärjestelmässä tieto liikkuu suoraan hallintalaitteelta väliaineen tai mekaanisen tehonsiirron kautta. Sähköisessä ja sähköhydraulisessa ohjausjärjestelmässä tieto komponenttien välillä liikkuu sähköisenä viestinä.

Tässä diplomityössä keskitytään sähköiseen ja sähköhydrauliseen ohjausjärjestelmään, joita käytetään nykyaikaisissa liikkuvissa työkoneissa. Sähköiset toimilaitteet ja tietoliikenne asettavat omat vaatimukset turvallisuussuunnittelulle, mitä käsitellään myöhemmin luvussa 3.3.

Ohjausjärjestelmä sisältää anturit, ohjausyksiköt ja hallintalaitteet. Antureiden tehtävä on kerätä tietoa koneen senhetkisestä tilasta. Mitattavia perussuureita ovat muun muassa paine, voima, nopeus, asema, kiihtyvyys, virtaus ja lämpötila, joita mitataan anturin tuntoelimen kautta. Mittausarvot muunnetaan mittamuuntimella mittausviestiksi, yleensä sähköjännitteeksi tai -virraksi. Mittausviesti muunnetaan mittalähtetimestä standardin mukaiseksi lähtöviestiksi. Ohjausjärjestelmän tehtävänä on muuttaa lähtöviesti mittaus-tulokseksi, jota käytetään järjestelmän anturitietona. [3.]

Anturitieto on muutettu muotoon, jota ohjausyksiköt voivat prosessoida. Ohjausyksiköt ovat pääsääntöisesti ohjelmoitavia logiikoita, joiden ohjelmointialusta on riippuvainen valmistajasta. Ohjausyksiköiden I/O-rajapinta ottaa vastaan anturien signaaleita ja lähettää komentokäskyjä toimilaitteille. Tulosignaaleina voidaan käyttää analogisia, digitaalisia tai pulssisignaaleja. Lähtösignaaleina ovat usein digitaaliset jänniteulostulot tai PWM-lähdöt (Pulse-Width Modulation). I/O-rajapintojen määrä vaihtelee ohjausyksikön tyypin mukaan. Lisäksi ohjausyksiköissä on sarjaväyläliitäntä ja nykyään yksi tai useampi väyläliitäntä.

Liikkuvien työkoneiden hallintalaitteet koostuvat ohjauspyörästä ja -sauvoista, kaas- ja jarrupolkimista ja suunnanvaihtimesta. Kaikkien hallintalaitteiden pohjalla on jokin anturi, joka lähettää tietoa ohjausyksikölle. Hallintalaitteet ja niiden käyttötarkoitukset ovat sovelluskohtaisia.

Sähköisen ohjausjärjestelmän hyödyt suhteessa mekaanishydrauliseen ohjausjärjestelmään ovat muun muassa

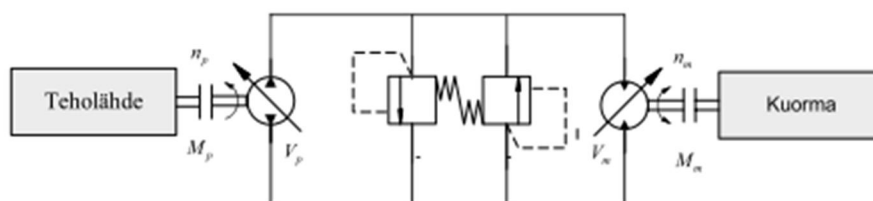
- vikojen paikannettavuus
- liikkuvan työkoneen toiminnan ennakoitavuus
- liikkeiden tarkkuus
- inhimillisten virheiden eliminointi.

Elektroniikan lisääntyessä järjestelmän tilan tarkkailu siirtyy aistihavainnoista ohjelmoitavan elektroniikan tekemään vertailuun. Elektroniikka tuo liikkuvaan työkoneeseen paljon etuja, mutta vaatii enemmän diagnostiikkaa ja lisää järjestelmän vikaantumistapoja. Tulevaisuudessa liikkuvan työkoneen ohjausjärjestelmään voidaan liittää simulointimalli, joka ei pelkästään kerro koneen sen hetkistä tilaa, vaan pystyy ennustamaan sen toimintaa.

2.2 Ajovoimansiirto

Ajovoimansiirto on järjestelmä, jolla käyttömootorin teho siirretään vetäville pyörille. Liikkuvilla työkoneissa ajovoimansiirto toteutetaan pääsääntöisesti mekaanisesti tai hydrostaattisesti. Mekaanisessa ajovoimansiirrossa moottorin kehittämä momentti ohjataan vetäville pyörille vaihteiston ja mekaanisen liitynnän kautta. Hydrostaattisen ajovoimansiirron edut ovat portaaton nopeuden säätö ja hyvä nopeus-momentti -suhde. Hydrostaattinen ajovoimansiirto on suljettu hydraulijärjestelmä, jossa väliaine kiertää pumpulta moottorille palaten takaisin pumpun imupuolelle (kuva 2).

Moottorin nopeutta ja pyörimissuuntaa muutetaan säätöventtiilivuoksisen pumpun avulla muuttamalla tilavuusvirran suuntaa ja suuruutta. Hydrostaattinen ajovoimansiirto koostuu yksinkertaisimmillaan käyttömootorista, hydraulipumpusta, hydraulimoottorista sekä letkuista ja putkista. Käyttömootorina liikkuvilla työkoneissa on usein dieselmoottori. Lisäksi järjestelmässä on paineenrajoitusventtiili, apupumppu, huuhteluventtiili ja mahdollisia säätöventtiileitä. Dieselmoottori pyörittää pumppua, ja toimilaitteena on hydraulimoottori. Näiden välille syntyy korkea- ja matalapainelinjat, joiden välissä ovat paineenrajoitusventtiilit. Apupumppu kompensoi vuotojen ja huuhtelukiertoon menevän tilavuusvirran. Huuhtelukierrossa väliaine poistuu huuhteluventtiilin, suodattimen ja jäähdyttimen kautta säiliöön. Lisäksi hydrostaattiseen ajovoimansiirtoon kuuluu ohjausjärjestelmän komponentteja. [2.]



Kuva 2 Hydrostaattisen ajovoimansiirron periaatekuva [2]

Hydrostaattisessa ajovoimansiirrossa dieselmoottorin tuottama momentti ja teho siirretään pumpun ja moottorin kautta pyörille. Momentti on verrannollinen paine-eroon hydraulikomponenttien yli, ja tehoon vaikuttavat lisäksi pyörimisnopeudet. Hydraulimoottoreita voi olla yksi, jolloin moottorin antama momentti ja teho jaetaan kaikkien pyörien kesken, tai jokaisella pyörällä voi olla oma napamoottorinsa. Perinteisen hydrostaattisen ajovoimansiirron lähtötilanteessa dieselmoottori pyörittää pumppua. Liikkeelle lähdettäessä pumpun ohjausta eli kulmaa lähdetään kasvattamaan. Hydraulimoottorien kulmat on ohjattu maksimiinsa. Liikkeelle lähdettäessä ja pienillä nopeuksilla ajaessa hydrostaattisen ajovoimansiirron momentti on suurimmillaan. Alla olevissa kaavoissa on osoitettu hydrostaattisen ajovoimansiirron välityssuhteet momentin ja pyörimisnopeuden suhteen. Oletuksena momenttia laskettaessa on, että paine-ero pumpun ja moot-

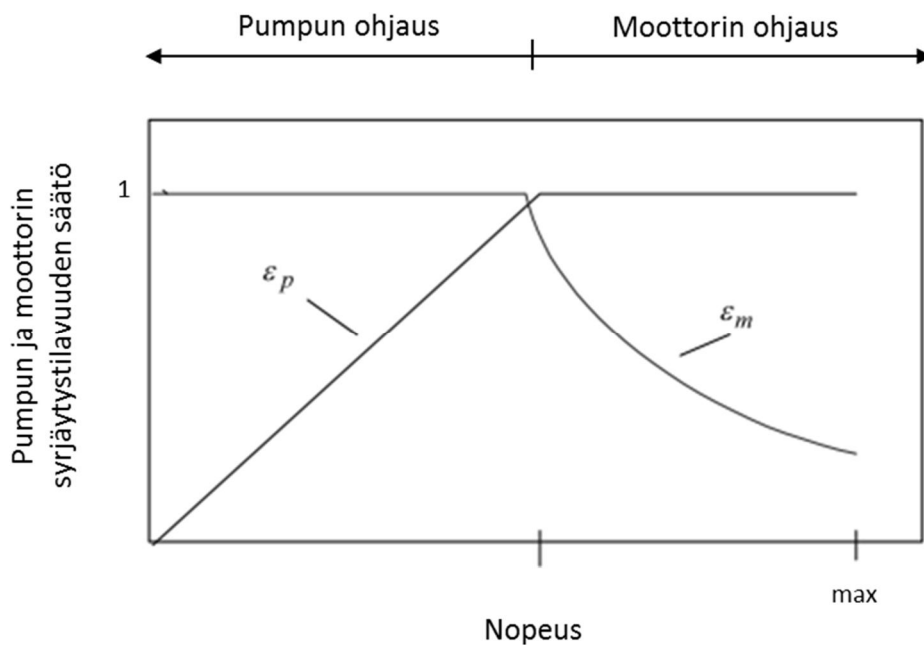
torin yli on sama ja pyörimisnopeuden kohdalla tilavuusvirta pumpulle ja moottorille on sama. [2.]

$$\frac{M_m}{M_p} = \frac{\varepsilon_m V_m}{\varepsilon_p V_p} \eta_{mhp} \eta_{mhm} \quad (1)$$

Nopeuden lisääntyessä pumpun kulma saavuttaa maksiminsa, minkä jälkeen moottorien kulmaa säädetään kohti minimiä, jolloin järjestelmän nopeus on suurimmillaan.

$$\frac{n_m}{n_p} = \frac{\varepsilon_p V_p}{\varepsilon_m V_m} \eta_{vp} \eta_{vm} \quad (2)$$

Hydrostaattista ajovoimansiirtoa ohjataan ohjausyksikön kautta. Kuvasta 3 nähdään pumpun ja hydraulimoottorin ohjausperiaate. [2.]



Kuva 3 Hydrostaattisen ajovoimansiirron ohjaus [2]

Hydrostaattisessa ajovoimansiirrosta käytetään pumppuna aksiaalimäntäpumppua tai pienillä teholuokilla hammaspyöräpumppua. Aksiaalimäntäpumppu on mäntäpumppu, jossa sylinterit on sijoitettu käyttöakselin suuntaisesti. Hydraulineeste, liikkuvissa työkohteissa hydraulioöljy, siirretään imuliitännästä paineliitännään mäntien edestakaisen liikkeen avulla. Mäntäpumppulla on hyvä hyötysuhde suurilla paineilla toimittaessa. Raken- teen ansiosta välykset saadaan pieniksi, ja vuodot kasvavat verrattain hitaasti paineen noustessa. Aksiaalimäntäpumppuissa on kiinteä tai pyörivä sylinteriryhmä, joka saa liik- keensä vinolevystä tai käyttöakselin ja sylinteriryhmän välisestä kulmasta. Tätä kulmaa

tai vinolevyn kulmaa säätämällä säädetään kierrostilavuutta. Vinolevypumppuja voidaan asentaa peräkkäin useampia, kun taas vinoakselipumpuissa ei ole läpimenevää akselia, joka mahdollistaisi useamman pumpun sarjaan kytkennän. [4.]

Hydrostaattisessa ajovoimansiirrossa hydraulimoottoreita voi olla vaihteleva määrä. Yksi moottori voi jakaa tuotetun hydraulien energian kaikille pyörille, kahdella moottorilla jaetaan hydraulien energia etu- ja taka-akseleille tai käytetään jokaiselle pyörälle omaa hydraulimoottoria eli napamoottoria. Hydrostaattisessa ajovoimansiirrossa käytetään aksiaalimäntämoottoreita tai hidaskäyntisiä radiaalimäntämoottoreita. Hydraulimoottoreiden tehtävänä on muuntaa hydraulinen teho takaisin mekaaniseksi pyörimisenergiaksi. Aksiaalimäntämoottorien ja -pumppujen rakenteet ovat lähellä toisiaan. Moottoreissa lisänä on vuotoliitäntä, joka mahdollistaa molempien käyttöliitännöiden kuormittamisen eli ajamisen molempiin suuntiin. [2.]

Hydrauliöljyn lämpiämisen ja epäpuhtauksien vuoksi suljetussa ajovoimansiirrossa on suodatuskierto. Huuhteluventtiili päästää hydrauliöljyn suodattimen ja jäädyttimen kautta tankkiin. Apupumppu korvaa menetetyn nesteen järjestelmään. Pumpun ja hydraulimoottorin väliin jääville korkea- ja matalapainelinjoille on omat paineenrajoitusventtiilit. Paineenrajoitusventtiilit sallivat läpivirtauksen, kun painetaso nousee yli asetetun raja-arvon. [2.]

2.3 Työhydrauliikka

Työhydrauliikalla toteutetaan liikkuvan työkoneneen työlaitteiden liikkeit. Toimilaitteina ovat yleisesti sylinterit tai hydraulimoottorit. Työhydrauliikassa hydraulijärjestelmä on yleisemmin avoimen piirin venttiiliohjattu järjestelmä. Avoimessa hydraulijärjestelmässä hydrauliöljy palaa toimilaitteelta säiliöön, josta se taas pumpun avulla imetään työkiertoon. Avoimen piirin hydraulijärjestelmä on yksinkertainen ja toteutukseltaan halvempi kuin suljettu piiri. Venttiiliohjatut järjestelmät perustuvat tilavuusvirran kuristamiseen, jolloin hyötysuhde jää matalaksi. [2.]

Avoin hydraulijärjestelmä voidaan jakaa vakioaine-, vakiotilavuusvirta- ja kuormantunteviin järjestelmiin. Eri järjestelmissä tehohäviöt syntyvät eri tilanteissa, ja on sovel-luskohtaista, mitä järjestelmää kannattaa käyttää. Vakioainejärjestelmässä pumpun kulmaa säädetään niin, että järjestelmän paine pysyy koko ajan samana. Tehohäviöitä syntyy silloin, kun kuorman paine on pieni ja tilavuusvirran tarve suuri tai kun kuorman paine ja tilavuusvirran tarve vaihtelevat. Vakiotilavuusvirtajärjestelmässä tilanne on päinvastainen: tilavuusvirran määrä pysyy vakiona, kun pumpun kierrostilavuus on vakio ja paine vaihtelee kuorman mukaan.

Tehohäviöt muodostuvat korkealla kuorman paineella ja pienellä tilavuusvirran tarpeella tai vaihtelevalla kuormanpaineella ja tilavuusvirralla. Kuormantuntevassa järjestel-

mässä kuormanpaine ohjaa tilavuusvirran säätöä. Pumpun paine ja tilavuusvirta saadaan vastaamaan toimilaitteen tarpeita ja tehohäviöt syntyvät ainoastaan komponenteissa. Kuormantuntevassa järjestelmässä hyötysuhde on hyvä kaikilla käyttötavoilla, ja siksi se on yleisimmin käytetty työhydrauliikan järjestelmä liikkuvissa työkoneissa. [2.]

Liikkuvan työkoneen työhydrauliikan peruskomponentit ovat pumpu, venttiilit, hydraulimoottori ja sylinterit. Komponenttien ominaisuudet määräytyvät liikkuvan työkoneen erityispiirteiden ja käyttötarkoituksen mukaan. Pumpu voi olla vakio- tai säätävä-tilavuuksinen. Pumpun tuottama teho ohjataan tarpeen mukaan ja usein tehon jakoa priorisoidaan. Suuntaventtiilit ohjaavat tilavuusvirran kulkua. Liikkuvissa työkoneissa työlaitteiden toimintaa ohjaavat suuntaventtiilit ovat usein venttiilipaketeissa, joissa on etu- ja päätylohkon lisäksi erinäinen määrä toimilaitelohkoja. Useimmiten suuntaventtiilit ovat proportionaali- tai servoventtiileitä, joita ohjataan sähköisesti. Suuntaventtiileitä voidaan ohjata portaattomasti ja saavuttaa sellainen asema, nopeus, voima tai momentti, joka halutaan. Ohjaustarkkuus riippuu suuntaventtiilin kyvystä seurata annettua suuretta. Servoventtiileissä on lisäksi takaisinkytkentä, joka seuraa tulo- ja lähtösuureen välis-
tä eroa ja yrittää pitää tämän mahdollisimman pienenä häiriötekijöistä huolimatta. [4.]

Venttiilipaketit mahdollistavat usean työlaitteen ohjaamisen samanaikaisesti. Etulohko sisältää liitännät pumpulle, esiohjauspaineelle ja tankkiin sekä mahdollisen liitännän kuormantuntosignaali (LS-signaali). Etulohkoon on sijoitettu usein myös paineenalennusventtiili, paineenrajoitusventtiili ja vastapaineventtiili. Päätylohkossa on liitännät pumpulle ja tankkiin sekä mahdolliset liitännän kuormantuntopaineelle ja esiohjaukselle. Toimilaitelohko sisältää itse suuntaventtiilin ja esiohjausventtiilin. Tämän lisäksi toimilaitelohkossa on painekompensaattori, sekä paineenrajoitusventtiilit toimilaitelinjoille ja kuormantuntolinjalle. Jokainen toimilaitelohko ohjaa jotain työlaitetta tai sen osaa. Toimilaitteena on sylinteri tai hydraulimoottori. Hydraulimoottorin muuttaessa hydraulisen tehon mekaaniseksi pyörimisliikkeeksi, muuttaa sylinteri hydraulisen tehon suoraviivaiseksi, edestakaiseksi liikkeeksi. Kaikissa hydraulijärjestelmissä komponentteja yhdistävät hydrauliletkut tai -putket, ja järjestelmissä on pääkomponenttien lisäksi erilaisia venttiileitä, suodattimia ja muita komponentteja.

2.4 Hydraulijärjestelmän luotettavuus

Hydraulijärjestelmien pääkomponentteja ovat pumpu, venttiilit, sylinteri sekä letkut ja putket. Hydraulijärjestelmien luotettavuus tarkoittaa järjestelmän kykyä toimia halutulla tavalla. Luotettavuudella tarkoitetaan myös sitä todennäköisyyttä, minkä ajan hydraulijärjestelmä toimii vaadituissa olosuhteissa. Hydraulikomponenttien vikaantumisessa on ominaista, että komponentin toimintakyky heikkenee. Järjestelmä ei ole enää luotettava, vaikka se näennäisesti toimisikin oikein. Tavallisimpia vikaantumisen tunnusmerkkejä ovat toimintahäiriöt, äänekkyyys, lämpeneminen, ryömiminen, värähtely ja ulkoinen vuo-

to. [5.] Vikaantuminen voi olla äkillinen satunnainen ilmiö tai seurausta pitkäaikaisesta ominaisuuksien heikkenemisestä. Äkillinen satunnainen vikaantuminen voi olla esimerkiksi venttiilin takertuminen liian ison partikkelin johdosta. Venttiilin sisäiset vuodot taas johtuvat usein pitkäaikaisesta ominaisuuksien heikkenemisestä kulumisen takia. [6.]

Hydrauliikkakomponenttien vikaantumisherkkyyttä kuvataan vikataajuudella (λ). Vikataajuus ilmoittaa odotetun vikaantumisajan. Hyvin koetelluille hydrauliikan komponenteille tämän ajan on yleensä ilmoitettu olevan 150 vuotta. Vikataajuus ei kuitenkaan ota huomioon erityisolosuhteita. Liikkuvissa työkoneissa käyttöolosuhteiden merkitys on huomattava komponenttien vikaantumisen suhteen. Hydrauliikan epäpuhtauksien on arvioitu olevan syynä noin 70 prosentissa kaikista hydrauliijärjestelmien vioista [7]. Järjestelmän epäpuhtaudet aiheuttavat komponenteissa kulumista, mikä vaikuttaa komponentin toiminta-arvoihin. Kulumisen ja toimintahäiriöt ovat vähäisiä, jos öljy voidaan pitää puhtaana. [8.] Käyttökokemukset osoittavat, että 2000-luvulla hydrauliijärjestelmien luotettavuus on parantunut. Tähän suurimpana syynä on ollut suodatuksen kehittyminen [6].

Henkilönostimien hydrauliikan toiminnan turvallisuuden ja luotettavuuden tutkimuksessa todetaan, että hydrauliikkaviat kehittyvät hitaasti, eivätkä luonteeltaan johda komponentin toimimattomuuteen. Siksi hydrauliikkavikojen korjaamista pitkitetään. [9.] Useimmat tutkimukset hydrauliijärjestelmien luotettavuudesta ovat prosessiteollisuuden puolelta. Liikkuvien työkoneiden kanssa olosuhteet ovat täysin erilaiset. Komponentit vikaantuvat samalla tavalla, mutta vikaherkkyys kasvaa. Esimerkiksi järjestelmään pääsee epäpuhtauksia huoltotöiden aikana, epätasainen alusta altistaa komponentit iskuille tai hankauksille, kosteus, lämpötila ja ympäristön olosuhteet. Liikkuvista työkoneista ei myöskään ole mitattua tietoa samalla tavalla kuin prosessiautomaation laitteista. Mittauslaitteistoja ei ole tehty liikkuvien työkoneiden olosuhteisiin ja laitteistot niihin ovat kalliita. [10.] Kattava, mutta vanha, ruotsalainen tutkimus metsäkoneiden vikaantumistapauksista on vuodelta 1977. Tutkimuksen mukaan huomattavasti eniten vikaantumistapauksia oli liitoselimissä. Sylinterien ja venttiilien vikaantumiset olivat seuraavaksi yleisemmät ongelmat. Moottoreissa ja pumpuissa vikaantumisia tapahtui harvoin. Tutkimuksen tuloksia on käsitelty Alatalon [11] Oulun yliopistossa tehdyssä raportissa. Uudempia kattavia tutkimuksia ei ole julkaistu. Kuitenkin liikkuvien työkoneiden huoltotöissä on huomattu letkujen kestävyysparantuneen samalla kun pumppujen ja moottorien kestoikä on heikentynyt.

Käyttövarmuus oikein asennetulla ja järjestelmään sopivalla hydraulikomponentilla on korkea. Komponenttien käyttöiän, jolloin se pystyy toimimaan edullisimmalla alueella, täytyisi olla lyhyempi kuin kestoian, eli vikaantumisajan. Hydraulikomponentit pitää huoltaa tai vaihtaa ennen kestoian umpeutumista. Kriittisyysmatriisilla (kuva 4.) arvioidaan komponentin vikaantumisen todennäköisyyttä ja seurausten vakavuutta. Vian va-

kavuustasoja ja vikojen ilmenemistodennäköisyyksiä on neljä. Mitä suurempi vakavuus ja vian ilmeneminen, sitä herkemmin komponentti on otettava huollon tarkkailuun. [12.]

Vian vakavuustaso

D Aiheuttaa erittäin vakavan konevaurion (peruskorjauksen tarve)	D-0	D-1	D-2	D-3
C Aiheuttaa koneen toiminnan pysähtymisen ja korjaaminen aiheuttaa tuotannon keskeyttämisen	C-0	C-1	C-2	C-3
B Aiheuttaa koneen toiminnan pysähtymisen, mutta on korjattavissa lyhyellä ajalla (< 2 h)	B-0	B-1	B-2	B-3
A Koneen toiminta häiriintyy, mutta sitä voidaan edelleen käyttää esim. seuraavaan suunniteltuun huoltoon	A-0	A-1	A-2	A-3
	0. Ei todennäköisesti ilmene	1. Ilmenee korkeintaan kerran	2. Esiintyy muutamia kertoja (< 10)	3. Esiintyy usein (> 10)

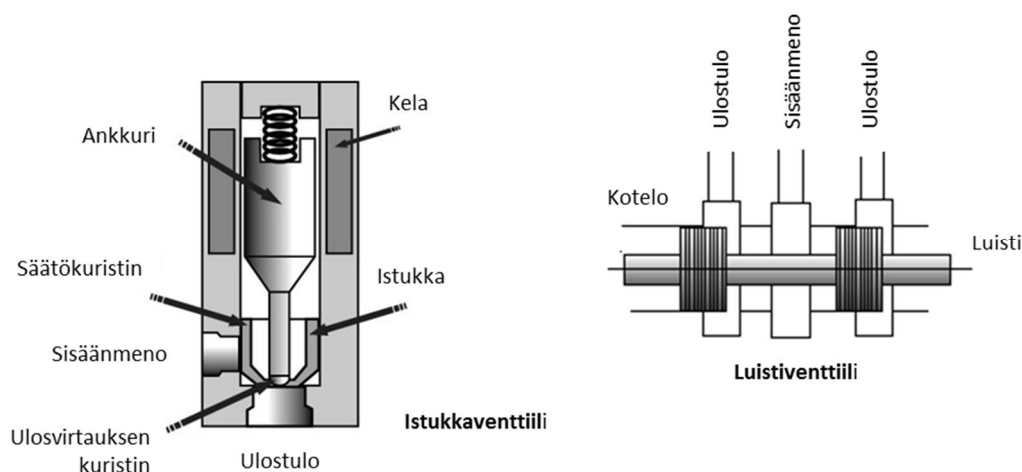
Vian esiintymistodennäköisyys koneen käyttöä aikana

Kuva 4 Vikakriittisyysmatriisi [12.]

Seuraavissa alikappaleissa käydään läpi hydraulikomponenttien vikaantumistapoja ja syitä kestoajan alenemiseen. Tarkasteltavat komponentit ovat sekä liikkuvien työkoneiden hydraulijärjestelmien kannalta olennaisia, että turvallisuuden näkökulmasta merkittävässä asemassa.

2.4.1 Venttiilit

Hydrauliventtiileillä toteutetaan energian ohjaus ja säätö. Venttiilit voidaan jakaa toimintojensa mukaan suunta-, virta-, paine- ja säätöventtiileihin. Suuntaventtiileillä ohjataan tilavuusvirran suuntaa ja vaikutetaan toimilaitteiden liikesuuntiin. Paineventtiileillä taas säädetään paineen suuruutta ja vaikutetaan toimilaitteista saataviin voimiin ja momentteihin. Toimilaitteilta saatavat voimat ja momentit riippuvat paineesta. Virtaventtiileillä säädetään tilavuusvirran suuruutta ja samalla toimilaitteiden liikenopeutta. Venttiilin toimintaa määrää sulkukappale, kara. Rakenteensa mukaan venttiilit voidaan jakaa joko luisti- tai istukkaventtiileihin (kuva 5). Luistiventtiileissä luisti liikkuu venttiilipesässä, sallien virtauksen portista toiseen. Istukkaventtiilissä kara painautuu istukkapintaa vasten ja avautuu ohjausvoimalla. Karan ohjausvoima on huomattavasti suurempi istukkatyyppisissä venttiileissä kuin luistityyppisissä. Istukkatyyppisessä venttiilissä on myös vähän sisäisiä vuotoja.



Kuva 5 Venttiilityypit

Venttiilit voidaan jaotella myös ohjaustapansa mukaan. Kaksitoimiset on-off -venttiilit ovat joko auki tai kiinni. Sähköisissä säätöventtiileissä eli proportionaalisissa venttiileissä, karaa voidaan avata ohjauskäskyn verran. Servoventtiileissä on lisäksi karan aseman takaisinkytkentä, jolloin karan ohjaus on tarkempi. [4.]

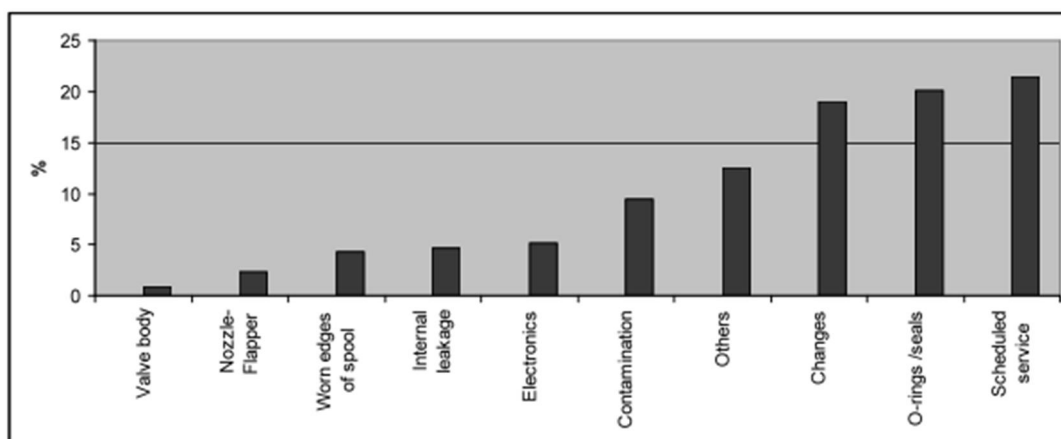
Erityyppisillä venttiileillä on omat vikaantumistapansa. Eri karatyyppin venttiileillä vikaantumiset poikkeavat karkeasti toisistaan. Luistityyppisillä venttiileillä vikaantumista aiheuttavat epäpuhtaudet, kun taas istukkatyyppisillä venttiileillä vikaantuminen aiheutuu tiivistyspinnan väsymiskulumista. Ohjaukseltaan kaksitoiminen venttiili kestää säätöventtiiliä paremmin hydrauliöljyn epäpuhtauksia. Tämä johtuu suuremmista välyksistä, käytön vähäisemmistä vaatimuksista ja suurista ohjausvoimista. Venttiileiden vikaantuminen johtuu ohjauskelojen, jousien tai tiivistimien vikaantumisesta. Jonkin verran venttiileissä on havaittavissa ohjausreunojen kulumista. [6.] Järjestelmän säätöventtiilien vaihtamisten yleisimmät syyt ovat määräraikaishuolto, o-rengas -tiivisteiden viat ja

muutokset venttiilin toiminnassa. Suoraan venttiilin vikaantumisesta johtuvia tilanteita ovat:

- epäpuhtaudet karan ja holkin välissä
- elektroniikan vikaantuminen
- karan ja/tai holkin kuluminen.

Epäpuhtaudet karan ja holkin välillä aiheuttavat äkillisiä komponenttien vikaantumisia. Komponenttien kuluminen on suoraan verrannollista öljyn epäpuhtauksien lukumäärään. Hiukkaset, jotka juuri ja juuri mahtuvat kiilautumaan venttiilin karan ja ohjauskanavan väliin, ovat vikaantumisen kannalta vaarallisimmat. Näissä tilanteissa vaurio ja ohjaushäiriö aiheutuvat välittömästi. [8.]

Venttiilin jumittuminen ja lietettyminen (silting) voivat aiheuttaa suurta vahinkoa niin koneelle kuin ihmisille. Toimilaitteiden pysähtyminen ja yllättävät liikkeet tai pysähtymättä jättäminen ovat seurausta epäpuhtauksista karan ja holkin välissä. Ohjauskelan vikaantuminen estää ohjauskäskyjen noudattamisen, ja integroidun elektroniikan vikaantuminen johtaa usein koko venttiilin vaihtoon. Tekniikan kehittyminen on vaikuttanut myös komponenttien kestoiän parantumiseen. Poikkeuksena tästä kehityksestä ovat kuitenkin sähköisesti ohjattavat venttiilit. Ilman sähköistä ohjausta olevien venttiilien käyttöikä on pidempi kuin sähköisellä ohjauksella varustettujen. Ilman sähköistä ohjausta venttiilin vikaantumismuotoja on vähemmän ja venttiilejä rasittava lämpökuorma on pienempi. [6.] Venttiilin kuluminen tapahtuu hitaasti ja johtuu hydraulijärjestelmän epäpuhtauksista. Kuluminen lisää sisäisiä vuotoja ja muuttaa venttiilin ominaisuuksia.



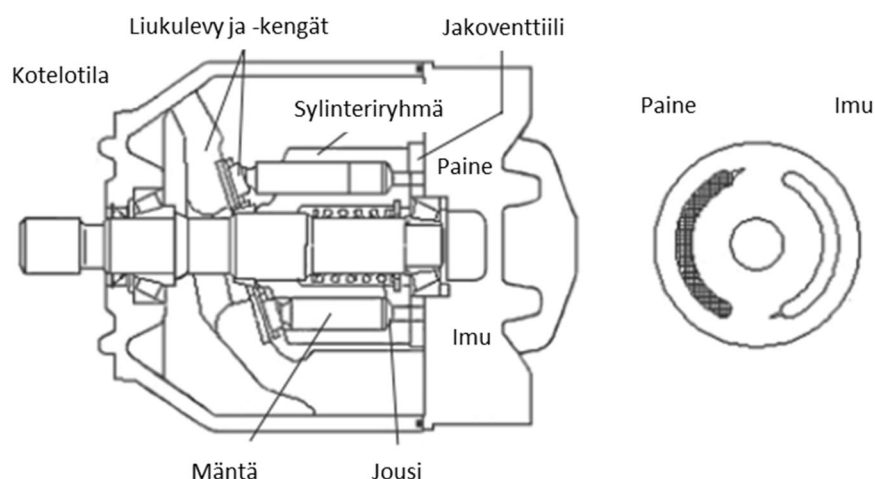
Kuva 6 Servoventtiileiden vaihtamiseen johtaneet yleisimmät syyt [10]

Kuvassa 6. on 4000 erityyppisen sähköohjatun venttiilin vaihtoon tai huoltoon johtaneita syitä. Yleisin syy on venttiilin määräaikaishuolto, mutta lähes yhtä usein venttiili huolletaan tiivisteen tai hydraulijärjestelmän muutoksien takia. Noin 10 % venttiileistä vaihdetaan järjestelmässä olleiden epäpuhtauksien takia. [10.] Hydraulikomponenttien kohdalla huollot ja komponenttien vaihdot tulee tehdä käyttöiän puitteissa. Silloin jär-

jestelmä toimii luotettavasti, eikä komponenttivaurioita ja niistä seuraavia vaarallisia tilanteita pääse syntymään.

2.4.2 Hydraulipumput ja toimilaitteet

Hydraulipumppujen kestoikään vaikuttaa järjestelmän paine. Liikkuviissa työkoneissa ajovoimansiirrossa paine on korkea, yleisimmin 30–35 MPa. Työhydrauliikassa painetaso vaihtelee sovelluksen mukaan. Eri pumpputyypin vikaantumistilanteet poikkeavat toisistaan pumpun rakenteen mukaan. Liikkuviissa työkoneissa käytetään usein aksiaalimäntäpumpua. Pumppuilla on korkea hyötysuhde sekä paineenkesto, ja pumppuja voi kytkeä samalle akselille useampia. Aksiaalimäntäpumpun poikkileikkaus on esitetty kuvassa 7. Mäntien vuoroittaisten imu- ja painejaksojen takia tilavuusvirta vaihtelee. Mitä enemmän mäntiä on, sitä tasaisempi on tilavuusvirta. Aksiaalimäntäpumpussa mäntiä on yleensä yhdeksän. Parittomalla määrällä mäntiä päästään samaan tulokseen kuin kaksinkertaisella parillisella määrällä. Männät nojaavat liukukenkien välityksellä liukulevyyn, joka on tietyssä kulmassa akseliin nähden. Liukukengät saavat voitelunsa suoraan käytettävästä hydrauliöljystä, ja öljyn puhtaus on suoraan verrannollinen liukukenkien kulumiseen. Akselia pyörittämällä saadaan aikaiseksi mäntien edestakainen liike, ja jakoventtiili jakaa paine- ja imuvaiheen. Sylinteriryhmän keskellä on voimakas jousi, joka muun muassa tiivistää jakoventtiilin ja sylinteriryhmän välisen vastinpinnan. Pinnan naarmuuntuminen aiheuttaa vuotoja kotelotilaan. Vuodot nostavat kotelopainetta, joka vaurioittaa tiivisteitä ja laakereita. Puhdas hydrauliöljy on aksiaalimäntäpumpujen luotettavuuden kannalta merkittävässä asemassa.



Kuva 7 Aksiaalimäntäpumpun rakenne [13]

Aksiaalimäntäpumppujen tyypilliset vikaantumistilanteet ovat:

- sisäiset vuodot kasvavien välyksien myötä
- liukukenkien pallokuppien kulumisen öljyn epäpuhtauksien takia
- kavitaation aiheuttama venttiililevyjen kuluminen
- kulmasäädön laakeroinnin vikaantuminen
- säätöventtiilin viat
- valmistus- ja materiaaliviat. [6; 13.]

Kavitaatio on ilmiö, joka aiheuttaa komponenttien pinnan kulumista. Kavitaatio syntyy, kun virtaavan nesteen paine alenee höyrystymispaineeseen. Esimerkiksi suuret virtausnopeudet, äkilliset virtauskanavan muutokset ja pumpun imusuodattimen aiheuttamat painehäviöt voivat saada aikaan paineen laskun, öljyn höyrystymisen ja lopulta komponentin pinnan vaurioitumisen kavitaatiokuplan romahtaessa kasaan. Suljetun piirin hydraulipumpuilla kavitaatiovaaraa pienentää sekä imu-, että painepuolella vaikuttava paine. Avoimen piirin pumpuilla kavitaatio voi aiheuttaa pumpun rikkoontumisen. Kavitaation seurauksena syntyneet paineiskut voivat irrottaa pumpun sisäpinnasta metallia. Kavitaatioeroosion seurauksena pumppu vaurioituu sekä kuluu, ja hydraulioöljyyn siirtyy metallipartikkeleita. [4; 6.]

Pumpuilla ja hydraulimoottoreilla vikaantumistilanteita ovat sisäiset tai ulkoiset vuodot, kiinnileikkaantuminen, alentunut hyötysuhde ja äänekkyyys. Vuotoihin syynä on kuluminen, jota tapahtuu epäpuhtauksien seurauksena, liian suuresta käyttöpaineesta tai huonontuneesta voitelusta. Kulumisen ja välyksien suurentuminen on syynä myös alentuneeseen hyötysuhteeseen. Huonontunut voitelu on kiinnileikkaantumisen suurin syy. Kova ääni on seurausta kavitaatioeroosiosta. Pumppujen määräaikaishuolloilla pyritään vähentämään ajan kuluessa tapahtuvaa vikaantumista. Äkillisiä vikaantumisia voivat aiheuttaa muun muassa materiaaliviasta johtuneet komponenttien hajoamiset. Komponenttien käyttöikä lisää oikein valittu ja kunnossa pidetty hydraulioöljy.

2.4.3 Letkut ja putket

Hydrauliletkun valintaan vaikuttavat järjestelmässä käytettävä hydraulineste ja sen lämpötila sekä paine. Letkukoko määräytyy painehäviöiden tai virtausnopeuden mukaan. [4.] Ympäristöolosuhteista lämpötila, kosteus ja mekaaniset rasitukset vaikuttavat valittavaan letkuun. Hydrauliletkun rakenne muodostuu sisäletkusta, välikerroksesta, vahvisteista ja kuoresta. Sisäletkun ominaisuudet valitaan hydraulinesteen ominaisuuksien ja lämpötilan mukaan. Vahvisteet valikoituvat paineenkeston sekä ulkoisten ja sisäisten voimien mukaan. Kuoren tehtävänä on suojata letkua ulkoisilta rasituksilta. Letkulle ilmoitetut ominaisuudet pätevät kun letkua ei taivuteta alle minimitaivutussäteen. Minimitaivutussäteet ja sallitut käyttöpaineet on ilmoitettu SAE-standardeissa. SAE (Society of Automotive Engineers) on Yhdysvaltalainen autoalan standardoimisjärjestö. Yleisimmät Suomessa käytetyt letkut ovat SAE J 517 standardin mukaisia. [14.]

Hydrauliputket ovat yleensä saumattuja tai hitsattuja hiiliteräsputkia. Putken paineenkestävyyttä määriteltäessä otetaan huomioon käyttöolot ja mahdolliset luokkavaatimukset, staattinen ja dynaaminen kuormitus sekä lämpötila. Hydrauliputkia taivuttaessa on myös huomioitava minimitaivutussäde, joka on 2,5 kertaa putken ulkohalkaisija. [14.] Standardi SFS 2230 [15] määrittelee saumattomille tarkkuusteräsputkille eri putkikoolle nimellispaineet, kierteet ja tiivistetason mitat. Putket mitoitetaan virtausnopeuden ja painehäviöiden mukaan. Putkissa voi syntyä resonanssi-ilmiö, jolloin järjestelmässä syntyvä melu on haitallista. Resonanssi-ilmiö syntyy, kun putken resonanssipituus on sama kuin pumpun ominaistaajuus. Putken resonanssia voidaan muuttaa paineakulla, letkulla tai putken pituutta muuttamalla. [14.]

Hydrauliletkujen ja putkien vikaantumista tarkasteltaessa, on otettava huomioon myös liittimet, joilla letkut ja putket liitetään muuhun järjestelmään. Hydrauliletkujen vikaantuminen tarkoittaa letkun puhkeamista, liittimen irtoamista tai sen kaulan katkeamista tai vuotoa letkussa tai liittimessä. Hydrauliputket vikaantuvat liittimen kohdalta. Hydrauliletkujen pääasiallinen vikaantuminen johtuu letkun virheellisestä valinnasta tai asennuksesta [6; 16]. Letkun rikkoutumisen syy on myös käyttöolosuhteissa. Liikkuvis- sa työkonelissa letkujen tukeminen ja suojaus voi olla hankalaa, jolloin aiheutuu murtumia ja kulumisia [11]. Uudemmassa käyttötutkimuksessa letkut koettiin hankalina käyttöön määrittämiseksi [6]. Putket ovat aina letkuja varmempia, mutta jäykän rakenteensa vuoksi ne eivät aina sovellu liikkuvan työkonteen rakenteeseen. Hydrauliletkujen oikea asennus on avainasemassa letkun kestävyys- kannalta. Hydrauliletku tulee kiinnittää oikein, eikä letkua saa taivuttaa yli sallitun taivutussäteen. Hydrauliletkujen reitit tulisi ottaa huomioon jo suunnitteluvaiheessa, jolloin niiden tarvitsema tila ja mahdolliset suojaukset voidaan suunnitella harkiten.

2.4.4 Suodattimet

Koska hydraulii- kan epäpuhtauksien aiheuttaessa suurimman osan hydraulii- kajarjes- telmien vikaantumisesta, ovat suodattimet avainasemassa luotettavuuden ja käyttövar- muuden parantamiseksi. Suodattimen suodatintarkkuus valitaan komponenttien pie- nimmän välyksen mukaan. [14.] Käyttökokemukset ovat osoittaneet, että suodattimen vaihtoväli ei määräydy vikaantumisen perusteella, mutta suodatin vikaantuu sitä her- kemmin mitä lähempänä suodattimen määräaika- vaihto on [6].

Suodattimet vaihdetaan joko määräajan kuluessa tai suodattimen yli vaikuttavan paine- eron noustessa yli sallitun tason. Paine- ero kasvaa suodatinelementtiin jääneiden epä- puhtauksien myötä. Suodatin poistaa epäpuhtauksia hydraulijärjestelmistä, mutta samal- la suodattimen vikaantumisen syy on epäpuhtaudet. Epäpuhtauksien pääseminen järjes- telmään suodattimen kautta johtuu vääränlaisen suodattimen valinnasta, suodattimen vaihtamisesta tai väärästä asennuksesta. Suodattimen tukkeutumista valvotaan anturilla.

Anturin vioittuminen tai huollon laiminlyönti voi johtaa suodattimen hajoamiseen ja epäpuhtauksien järjestelmään pääsemiseen.

Suodattimen tehokkuus riippuu suodattimen läpäisevien hiukkasten koosta ja määrästä. Suodattimen tarkkuus riippuu komponenttien pienimmästä välyksestä, samoin komponenttien kestoikää voidaan kasvattaa tiheämmällä suodattimella. Suodattimia on järjestelmässä erilaisissa sijoituskohteissa. Imusuodattimet ovat pumpun imupuolella, painesuodattimet pumpun ja toimilaitteen välillä. Palusuodatin on toimilaitteen ja säiliön välillä. Lisäksi järjestelmässä voi olla erillinen suodatuskierto. Muita suodattimia ovat ilmansuodatin ja öljytäytön suodatin. [14.]

3 KONEIDEN TURVALLISUUTTA KOSKEVAT SÄÄDÖKSET

Vuosina 1985–2007 Suomessa on tapahtunut 97 kuolemaan johtanutta tapaturmaa, joissa liikkuva työkone oli osallisena [17]. Yleisimmin tapaturmat ovat olleet käyttäjän huolimattomuudesta tai yllättävästä käynnistymisestä johtuvia. Työkoneiden huollon ja vianetsinnän aikana tapahtuu hydraulikasta johtuvia työtapaturmia. Liikkuvassa työkooneessa sivullisten loukkaantumisriski on korkea, koska vaara-alue liikkuu ja muuttuu työkooneen mukana. Koneiden valmistaja on vastuussa siitä, ettei kone aiheuta henkeä tai terveyttä uhkaavaa vaaraa henkilöille tai ympäristölle. Koneiden vaatimustenmukaisuus on pystyttävä osoittamaan sitä vaadittaessa niin Suomessa kuin vientimaassa.

Koneiden suunnittelua ja valmistusta valvoo laki eräiden teknisten laitteiden vaatimustenmukaisuudesta - yleisemmin puhuttuna konelaki 1016/2004 [18]. Lain tarkoituksena on varmistaa, että kone tai muu tekninen laite on vaatimusten mukainen, eikä aiheuta valmistajan tarkoittamassa käytössä tapaturman vaaraa eikä terveyden haittaa. Konedirektiivi 2006/42/EY [19] velvoittaa jäsenmaita muuttamaan oman lainsäädännön direktiivin mukaiseksi. Sekä lain että direktiivin vaatimukset on pantu täytäntöön valtioneuvoston asetuksella koneiden turvallisuudesta 400/2008 [20].

Yhdenmukaiset harmonisoidut eurooppalaiset standardit auttavat tulkitsemaan direktiivin ja koneasetuksen olennaisia vaatimuksia. Kun kone tehdään standardien mukaisesti, oletetaan sen täyttävän lain vaatimukset [21]. Valtioneuvoston asetus koneiden turvallisuudesta koskee koneita, vaihdettavia laitteita, turvakomponentteja ja osittain valmiita koneita. Asetusta ei sovelleta traktoreihin tai moottoriajoneuvodirektiivin alaisiin ajoneuvoihin lukuun ottamatta näihin liitettäviä lisälaitteita. Koneasetuksen liitteessä I on kerrottu koneen suunnittelua ja rakentamista koskevat olennaiset terveys- ja turvallisuusvaatimukset [21]. Liitteen kohdassa kolme on lueteltu erikseen lisävaatimuksia liikkuvalle työkooneelle.

Terveys- ja turvallisuusvaatimukset ovat pakollisia säädöksiä, joiden tarkoitus on varmistaa henkilöiden terveys ja turvallisuus sekä omaisuuden että tietyltä osin ympäristön suojele. Koneen valmistaja on vastuussa koneen turvallisuudesta, ja tarvittaessa tämän on pystyttävä osoittamaan koneen vaatimustenmukaisuus. Koneen valmistajan on allekirjoitettava vaatimustenmukaisuusvakuutus, jonka sisältö käy ilmi koneasetuksen liitteestä II. Esimerkki vaatimustenmukaisuusvakuutuksesta on tämän diplomityön liitteessä 1. Koneiden turvallisuutta valvovat työsuojeluviranomaiset. Sosiaali- ja terveysminis-

terion työsuojeluosasto voi antaa määräykset tietyn koneen myynnin kieltämisestä, poisvedosta ja korjausvelvoitteista. Vakavan tapaturman sattuessa asia viedään lähes aina oikeuden käsiteltäväksi. Näiden tahojen lisäksi koneen jälleenmyyjä, ostaja tai käyttäjä voi aina vaatia nähtäväksi koneen teknisen tiedoston joka osoittaa, että kone on koneasetuksen mukainen. Teknisen tiedoston sisältämät tiedot ja dokumentit on kirjattu koneasetuksen liitteeseen VII, ja tämän diplomityön liitteeseen 2. Koneen tekninen tiedosto on oltava viranomaisten käytössä vähintään kymmenen vuoden ajan. Teknisen tiedoston ei tarvitse olla jatkuvasti käytettävissä aineellisessa muodossa, mutta se on pystyttävä kasaamaan määräajassa. Jos teknistä tiedostoa ei voida esittää viranomaiselle määräajassa, voidaan sitä pitää riittävänä todisteena sille, että kone ei täytä terveys- ja turvallisuusvaatimuksia. [20.]

Valmistettavien koneiden tulee täyttää koneasetuksen vaatimukset. CE-merkintä on valmistajan vakuutus siitä, että kone vastaa Euroopan Unionin lainsäädäntöä. Merkintä osoittaa, että valmistaja ottaa kaiken vastuun koneen vaatimusten mukaisuudesta. CE-merkintä ei kuitenkaan vielä takaa koneen turvallisuutta. Se on merkki siitä, että kone on arvioitu ennen kuin se on laskettu markkinoille. CE-merkinnän väärinkäytön vuoksi vasta vaatimustenmukaisuusvakuutus antaa jonkinlaisen takeen siitä, että kone on turvallinen. CE-merkintärikkomuksista on säädetty oma laki (187/2010), jota sovelletaan niihin CE-merkintärikkomuksiin, joita ei muualla lainsäädännössä huomioida. Vain CE-merkitty kone voidaan saattaa markkinoille ja ottaa käyttöön. [22.]

Jos valmistaja ei pysty osoittamaan koneen vaatimustenmukaisuutta dokumentein, on valmistaja yksin vastuussa ja korvausvelvollinen tapaturman sattuessa. Jälkikäteen vaatimustenmukaisuuden osoittaminen on lähes mahdotonta. Yhtä vaikeaa on osoittaa huonosti dokumentoidusta riskienhallinnasta, mitkä vaaralliset tilanteet ja käyttötapaukset on huomioitu koneen suunnittelussa. Turvallisuussuunnittelun tulisi olla alusta lähtien osa laadukasta koneensuunnittelutyötä, joka tuottaa tarvittavat dokumentit suunnittelun edetessä. Koneasetus ja siihen liittyvät standardit tulee seurata konetta koko sen elinkaaren ajan.

3.1 Standardit

Standardit eivät ole pakottavia määräyksiä, vaan ne tukevat direktiivien ja asetusten vaatimuksia. Standardit kuvaavat yksityiskohtaisemmin koneasetuksen teknisiä ratkaisuja. Direktiiveihin liittyvät harmonisoidut eli yhdenmukaistetut standardit. Eurooppalaiset standardit merkitään tunnuksella EN ja julkaistaan Suomessa tunnuksella SFS-EN. Jos nämä eurooppalaiset standardit ovat yhdenmukaisia kansainvälisen standardin

Standardinumero	Kuvaus
A-tyypin standardit	
SFS-EN ISO 12100	Koneturvallisuus. Yleiset suunnitteluperiaatteet
SFS-EN ISO 14121	Koneturvallisuus. Riskin arviointi
B-tyypin standardit	
SFS-EN 894-3	Koneturvallisuus. Osa 3 Ohjaimet
SFS-EN 953	Koneturvallisuus. Suojukset. Kiinteiden ja avattavien suojusten suunnittelun ja rakenteen yleiset periaatteet.
SFS-EN 1037	Koneturvallisuus. Odottamattoman käynnistymisen estäminen
SFS-EN 1093	Koneturvallisuus. Vaaraa aiheuttavien ilmassa kulkeutuvien aineiden päästöjen arviointi.
SFS-EN 1837	Koneturvallisuus. Koneiden valaistus
SFS-EN ISO 4413	Hydraulinen tehonsiirto
SFS-EN 13478	Koneturvallisuus. Palontorjunta ja palosuojelu
SFS-EN ISO 13849	Koneturvallisuus. Ohjausjärjestelmä
SFS-EN ISO 13850	Koneturvallisuus. Hätäpysäytys
SFS-EN ISO 13855	Koneturvallisuus. Suojausteknisten laitteiden sijoitus ottaen huomioon kehon osien lähestymisnopeudet
SFS-EN ISO 13857	Koneturvallisuus. Turvaetäisyydet yläraajojen ja alaraajojen ulottumisen estämiseksi vaaravyöhykkeillä
SFS-EN ISO 14119	Koneturvallisuus. Suojusten kytkentä koneen toimintaan
SFS-EN ISO 14121-1	Koneturvallisuus. Riskin arviointi.
SFS-ISO/TR 14121-2	Koneturvallisuus. Riskin arviointi.
SFS-EN ISO 14122	Koneturvallisuus. Koneiden kiinteät kulkutiet.
SFS-EN ISO 60204	Koneturvallisuus. Koneiden sähkölaitteisto
SFS-EN 61310	Koneturvallisuus. Merkinantaminen, merkitseminen ja vaikuttaminen.
SFS-EN 61508-1	Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1. Yleiset vaatimukset
SFS-EN 62601	Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus
C-tyypin standardit	
SFS-EN 474	Earth-moving machinery
SFS-EN 809	Pumput ja pumppuyksiköt nesteille
SFS-EN ISO 4254	Agricultural machinery
SFS-EN 500	Mobile road construction machinery
SFS ISO 4557	Maansiirtokoneen. Kaivukoneet. Hallintalaitteet

Taulukko 1 Liikkuvan työkoneneen turvallisuusstandardeja

kanssa, niiden tunnus on SFS-EN ISO. Standardeista poikkeavia ratkaisuja voidaan käyttää, jos pystytään osoittamaan, että näillä ratkaisuilla päästään samaan turvallisuustasoon [21]. Yhdenmukaistettuja standardeja noudattamalla täytetään koneen turvallisuutta koskevat säädökset, muun muassa koneasetuksen liitteen 1 mukaiset yleiset terveys- ja turvallisuusvaatimukset.

Koneasetusta täydentävät kolme eritason standardityyppiä. A-tyypin standardit koskevat kaikkia koneita, ja sisältävät yleisiä suunnitteluperiaatteita koskevia määrittelyjä. B-tyypin standardit koskevat tiettyä ominaisuutta tai turvalaitetta. Standardit voivat käsitellä myös joitain usealle koneelle yhdenmukaisia ominaisuuksia. B-tyypin standardit kuvaavat usein luokkia tai tyyppejä, joiden mukaan eri ominaisuuksia valitaan. Standardeissa ei kuitenkaan kerrota, mikä luokka tai tyyppi on valittava. C-tyypin standardit koskevat tiettyä konetta tai koneryhmää. Näissä standardeissa saatetaan myös mainita B-tyypin standardin luokka tai tyyppi, joka tulee kyseiseen koneeseen valita. Jos valmistettavasta koneesta on olemassa C-tyypin standardi, sitä kannattaa noudattaa. Muutoin valinnat tehdään yleisempien standardien mukaan. Ylemmän tason vaatimuksia ei toisteta alemman tason standardeissa. [21.]

Taulukossa 1 luetellaan eri tason standardeja, joita voidaan käyttää liikkuvan työkonen turvallisuussuunnittelussa. Taulukossa nimettyjen standardien lisäksi on olemassa useita esimerkiksi ergonomiaa, melua ja mekaanista värähtelyä koskevia standardeja, joista löytyy ohjeistusta koneenrakennukseen. Kaikki standardit on saatavissa Suomen Standardoimisliiton kautta.

3.2 Yleiset suunnitteluperiaatteet

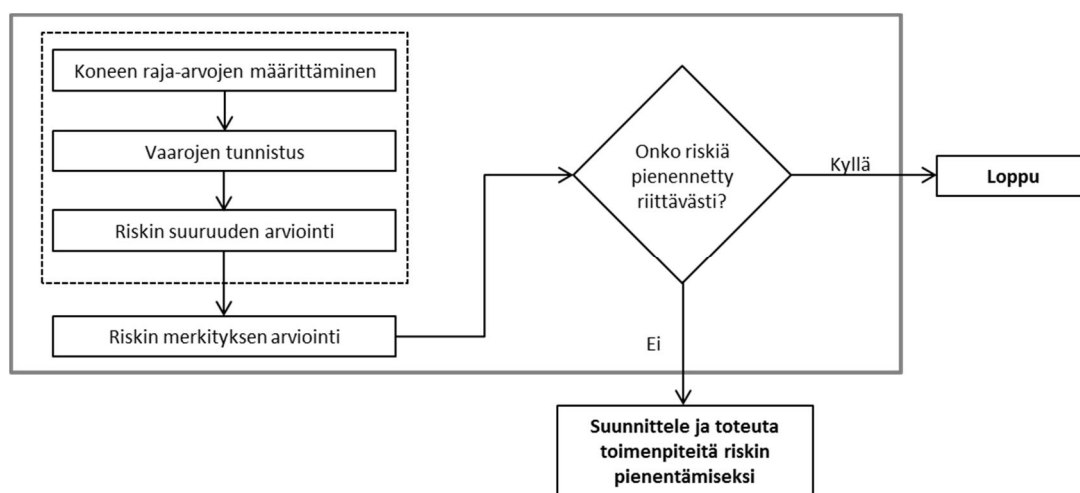
SFS-EN ISO 12100 standardissa [23] esitellään yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. Standardi määrittelee peruskäsitteet, periaatteet ja menetelmät turvallisuuden aikaansaamiseksi koneita suunniteltaessa.

Koneasetuksen liitteessä I sanotaan ”Koneen valmistajan tai tämän valtuutetun edustajan on varmistettava, että tehdään riskin arviointi, jotta koneeseen sovellettavat terveys- ja turvallisuusvaatimukset voidaan määrittää. Kone on sen jälkeen suunniteltava ja rakennettava ottaen huomioon riskin arvioinnin tulokset.” [20, liite I.] Riskin arviointi on turvallisuussuunnittelun lähtökohta. Riskin arvioinnin työväline on riskianalyysi, joka pitää sisällään raja-arvojen määrittämisen, vaarojen tunnistamisen ja riskin suuruuden arvioinnin.

$$\text{Riski} = \text{Tapahtuman taajuus} \times \text{vaarallisen tapahtuman seuraus}$$

Riski muodostuu ajateltavissa olevasta seurauksen vakavuudesta ja todennäköisyydestä. Standardin SFS-EN ISO 12100 mukaan riskin arviointiin ja pienentämiseen kuuluu viisi vaihetta (kuva 8).

- Määritetään koneen raja-arvot, joihin sisältyvät tarkoitettu käyttö ja kohtuudella ennakoitavissa oleva väärinkäyttö.
- Tunnistetaan vaarat ja niihin liittyvät vaaratilanteet.
- Arvioidaan riskin suuruus kunkin vaaran ja vaaratilanteen osalta
- Arvioidaan riskin merkitys ja tehdään päätöksen riskin poistamiseksi
- Poistetaan vaara tai pienennetään vaaraan liittyvää riskiä suojaustoimenpiteiden avulla



Kuva 8 Riskin arvioinnin ja pienentämisen menetelmä [20]

Koneen raja-arvojen määrittäminen, vaarojen tunnistus ja riskin suuruuden arviointi kuuluvat riskianalyysiin, joka tulee tehdä jokaisesta koneesta, ja sitä on tarkennettava koko koneen elinkaaren ajan, jos käyttökokemukset tai tapaturmat antavat siihen aihetta.

3.2.1 Koneen raja-arvot

Raja-arvojen määrittelyn tavoitteena on saada aikaan selkeä kuvaus koneen mekaanisista ja fyysisistä ominaisuuksista, sekä toiminnallisesta suorituskyvystä. Raja-arvot sisältävät kuvauksen koneen tarkoitetusta käytöstä ja ennakoitavissa olevasta väärinkäytöstä, sekä toimintaympäristöstä, jossa konetta käytetään. Ominaisuudet tulee määritellä siten, että niihin liittyvät vaaratekijät voidaan tunnistaa. Koneesta tulee ilmoittaa käyttötapa, koko, massa, suurimmat liikenopeudet ja koneen synnyttämät päästöt. Koneesta ilmoitetaan myös sen käyttämät energiat (esimerkiksi sähkö ja hydraulikka), sekä niiden ominaisuudet (jännite, paine). Lisäksi määritellään koneen automaatioaste ja ihmisen tehtävät konetta käytettäessä. Taulukossa 2 on esimerkki, kuinka raja-arvot voidaan jakaa.

Käyttörajat	<ul style="list-style-type: none"> • Koneen käyttötavat ja käyttöympäristö • Käyttäjien puuttuminen toimintaan, myös toimintahäiriöihin • Koneen käyttäjien koulutustaso, kokeneisuus, kyvyt • Muiden ihmisten altistuminen vaaroille
Tilarajat	<ul style="list-style-type: none"> • Koneen liikkeiden laajuus • Koneen käyttäjän vaatima tila • Käyttäjä-kone rajapinta • Kone-tehonsyöttö rajapinta
Aikarajat	<ul style="list-style-type: none"> • Koneen ja sen osien käyttöikä • Huoltovälit
Muut raja-arvot	<ul style="list-style-type: none"> • Käsiteltävien materiaalien ominaisuudet • Puhtaanapitoon liittyvät vaatimukset • Käyttöympäristön olosuhteiden raja-arvot

Taulukko 2 Koneen huomioitavat raja-arvot [23.]

Koneen käyttäjiin luetaan kuljettajan lisäksi kunnossapidon henkilöt, tekniset asiantuntijat, harjoittelijat ja muut koneen kanssa kosketuksiin joutuvat henkilöt. Raja-arvot, samoin kuin vaarojen tunnistaminen, on määriteltävä kaikille koneen elinkaaren vaiheille. Koneen elinkaari sisältää kuljetuksen, kokoonpanon, asennuksen, käyttöönoton, käytön sekä purkamisen, käytöstä poiston ja romuttamisen. Riskin arvioinnin tulisi perustua todelliselle ymmärrykselle koneen raja-arvoista ja funktioista. [23.]

3.2.2 Vaarojen tunnistaminen

Vaarojen tunnistaminen on järjestelmällistä vaaratilanteiden läpikäymistä. Vaara ymmärretään henkeä tai terveyttä uhkaavan vahingon lähteenä. Vaaratilanteet on tunnistettava ihmisen ja koneen kaikissa vuorovaikutustilanteissa koneen elinkaaren ajan. Katava vaaratilanteiden tunnistaminen on pohjana onnistuneelle riskianalyysille. Vaarojen tunnistamisen apuna voi käyttää niin tilastotietoa, samankaltaisten koneiden käyttökokemuksia, eri alojen asiantuntijoita ja standardien ohjeistuksia.

Standardissa SFS-EN ISO 12100 liitteessä B on esimerkkejä vaaroista, vaaratilanteista ja vaarallisista tapahtumista, jotka toimivat tarkastuslistana koneille, joille ei ole C-tyypin standardia. Siirilä [21] on koonnut standardeista luettelon kaikkia koneita koskevista yleisistä vaaratilanteista:

- mekaaniset vaaratekijät
- odottamaton käynnistyminen tai muu toiminto
- energiansyötön vika
- ohjauspiirin vika
- asennusvirheet
- putoavat tai sinkoutuvat osat tai nesteen/kaasun purkautuminen
- henkilön liukastuminen, kompastuminen putoaminen.

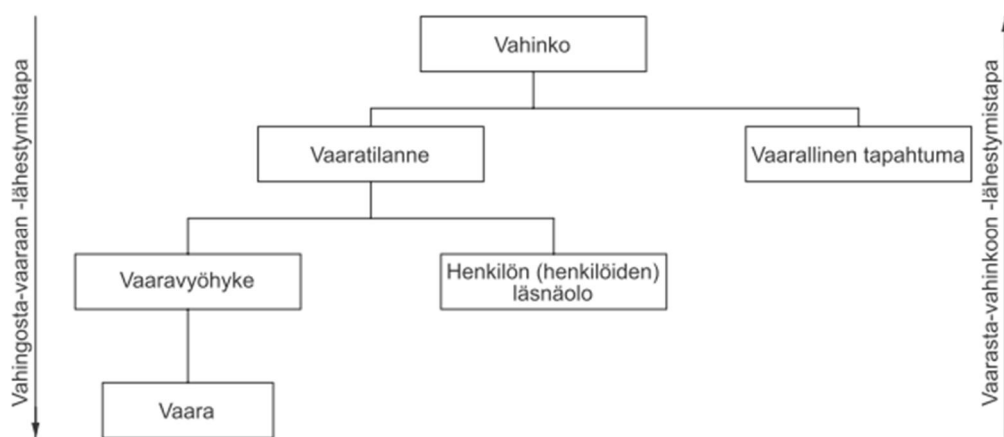
Liitteen B mukaan mekaanisia vaaroja voivat olla muun muassa:

- puristuminen
- leikkautuminen
- kiinnijääminen
- isku
- viilto
- hankautuminen
- korkeapaineisen nesteen injektointuminen.

Lisäksi liikkuvia työkoneita koskevia erityisiä vaaroja ovat:

- koneen kulkemiseen liittyvät vaarat, esimerkiksi yllättävä liikkeelle lähteminen moottoria käynnistettäessä
- liikkuvien koneiden ohjaamoon tai muuhun työskentelypaikkaan liittyvät vaarat
- koneen kaatumisvaara
- varastoitunut energia.

Vaarojen tunnistamisen tulisi tuottaa lista vaaroista, vaaratilanteista ja vaarallisista tapahtumista, jotka voivat johtaa vahinkoon. Standardissa SFS-EN ISO 14121 [24] pääta-son lähtökohtana käytetään joko ”vahingosta–vaaraan” tai ”vaarasta–vahinkoon” – lähestymistapaa (kuva 9).



Kuva 9 Vahingosta - vaaraan ja vaarasta - vahinkoon lähestymistavat [24]

Vahingosta–vaaraan -lähestymistavassa otetaan alkutilanteeksi mahdollisten seurausten tarkastuslista ja selvitetään mitkä tilanteet voisivat vahingon aiheuttaa. Vaarasta–vahinkoon -lähestymistavassa taas liikkuvan työkoneen kaikkia mahdollisia vaaratilanteita tarkastellaan ja arvioidaan, millaisen vahingon nämä vaaratilanteet voisivat aiheuttaa.

Vaarojen tunnistamiseen voidaan käyttää useita tapoja ja menetelmiä. Kaikki menetelmät eivät sovi suoraan koneiden aiheuttamien vaarojen tunnistamiseen. Yleisimmin käytetyt menetelmät ovat vika- ja vaikutusanalyysi (VVA) ja poikkeamatarkastelu (HAZOP). Vaarat on tunnistettava erilaisissa koneen käyttötilanteissa, ja häiriötilanteissa koneen elinkaaren aikana. Ihmisen toiminta näissä tilanteissa sekä koneen oletettavissa oleva väärinkäyttö tulee sisällyttää vaarallisten tilanteiden arviointiin. Vaarojen tunnistamista ei pidä rajoittaa millään muotoa, vaan vaarojen tunnistamisen tulisi olla vapaata ideointia kaikista mahdollisista näkökulmista. Vasta riskin suuruuden arviointi osoittaa ne vaaratilanteet, jotka vaativat toimenpiteitä.

3.2.3 Riskin suuruuden arviointi

Vaarojen tunnistamisen jälkeen voidaan arvioida vaarasta aiheutuvan riskin suuruus. Riskin suuruuteen vaikuttavat tapahtuman todennäköisyys ja seurauksen vakavuus. Riskin seurausten ja todennäköisyyksien arvioinnin menetelmiä on useita. Menetelmiä esitellään teknisessä raportissa SFS-ISO/TR 14121-2 [25]. Raportissa esitetään riskin arviointia käytännössä. Riskin suuruuden arvioinnissa käytetään usein kolmiportaista luokitelua. Haitan vakavuus voi olla lievä, vaikea tai suuri, ja esiintymistodennäköisyys epätodennäköinen, mahdollinen tai todennäköinen (kuva 10).

Todennäköisyys	Seuraukset		
	Lievä	Vaikea	Suuri
Epätodennäköinen	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski
Mahdollinen	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
Todennäköinen	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski

Kuva 10 Kolmiportainen riskitaulukko

Kolmiportaisen riskitaulukon viisi eri riskiluokkaa ohjeistavat miten eri luokkien riskeihin tulee suhtautua. Luokkien 1 ja 2 kohdalla välitöntä toimenpidettä ei tarvita. Luokassa 3 riskin pienentämiseksi tarvitaan toimenpiteitä, mutta ne voidaan tehdä tietyn aikarajan puitteissa. Merkittävän riskin (luokka 4) ollessa kyseessä, riskiä on pienennettävä välittömästi, eikä mahdollista meneillään olevaa työtä saa jatkaa, ennen kuin riski on siedettävällä tasolla. Sietämätön riski (luokka 5) lopettaa mahdollisen työn heti. Ellei riskiä saada pienennettyä tarpeeksi, on koneen pysyttävä käyttökiellossa. [21.] Koneturvallisuuden näkökulmasta on tärkeä tietää ja dokumentoida, kuinka tiettyyn riskiluokkaan päädytään. Luvussa 4.1. esitellään tarkemmin riskiluokan valintaan vaikuttavia tekijöitä.

3.2.4 Riskin merkityksen arviointi

Riskin merkityksen arviointi on prosessi, jossa tehdään päätökset riskien siedettävyydestä eli siitä minkälaiset riskit on hyväksyttävä. Seurauksen vakavuuteen vaikuttavat haitan luonne, laajuus, palautuvuus ja kesto. Lisäksi arvioidaan onko haitan vakavuus lievä, vaikea vai voiko se aiheuttaa esimerkiksi henkilön kuoleman. On arvioitava onko haitalle alttiina yksi vai useampi henkilö. Riskin merkitykseen vaikuttaa palautuuko vammasta tai terveyshaitasta, vai onko kyseessä esimerkiksi kehonosan menettäminen. Lisäksi vakavuuteen vaikuttaa, kuinka taajaan haitalle ollaan altistuneita. [23; 24; 25.]

Vahingon todennäköisyyteen vaikuttaa, kuinka henkilöt ovat altistuneina vaaroille, mikä on vaarallisten tapahtumien esiintymisen laajuus ja tiheys, sekä voidaanko vahingon tapahtumista ennakoida tai ehkäistä. Pelkästään riskin suuruus ei saa olla ainoa kriteeri päätettäessä iteratiivista riskin pienentämisprosessia. Pienellä, mutta usein esiintyvällä riskillä, voi olla merkittäviä vaikutuksia. Vaarallisten tapahtumien esiintymisen todennäköisyydestä saamme tietoja esimerkiksi tapaturmatilastoista ja käyttökokemuksista. [23; 24; 25.]

3.2.5 Riskin pienentäminen

Riskin arvioinnin tulosten mukaan suunnittelijan on päätettävä toimenpiteistä riskin poistamiseksi tai pienentämiseksi. On pohdittava, onko tarpeen muuttaa jotain koneen perusominaisuutta, ja voidaanko riski poistaa luontaisilla suunnittelumenetelmillä. Jos riskin poistaminen kokonaan ei ole mahdollista, on riskiä pienennettävä suojaustoimenpiteillä.

Riski on ensisijaisesti poistettava, tai sitä on pienennettävä, luontaisesti turvallisilla suunnittelutoimenpiteillä. Kone suunnitellaan niin, ettei vaaratilannetta pääse tapahtumaan. Hydraulikan osalta turvallisista suunnittelutoimenpiteitä ovat:

- painerajojen käyttö, jolloin suurinta suunniteltua painetta ei ylitetä
- vuodot tai komponenttiviatiat eivät saa aiheuttaa vaarallista korkeapaineista nestesuihkua
- säiliöiden suunnittelussa noudatetaan standardien ohjeita
- komponentit, erityisesti putket ja letkut, suojataan haitallisilta ulkoisilta vaikutuksilta
- koneen irrottaminen tehonsyötöstä tyhjentää myös varastoituneen energian
- paineistetuksi jääneet osat osoitetaan selvillä merkeillä ja paineenpurkulaitteilla [23; 26].

Jos suunnittelulla ei saavuteta tarpeellista turvallisuustasoa, on käytettävä suojaustoimenpiteitä tai täydentäviä suojaustoimenpiteitä. Jäännösriskit, eli ne riskit joita ei voida suunnittelulla eikä suojaustoimenpiteillä poistaa, täytyy osoittaa koneen käyttöä koske-

vissa tiedoissa turvamerkinnoin ja varoituksin. Jäännösriskit tulee käydä läpi mahdollisessa käyttökoulutuksessa tai käyttöohjekirjassa. [23.]

Kun muutokset riskin poistamiseksi tai pienentämiseksi on päätetty, on riskit arvioitava uudelleen, ja varmistettava etteivät muutokset tuo mukanaan uusia riskejä. Riskin arvioinnista ja riskien pienentämisen menettelyistä tulee tehdä asiaankuuluvat dokumentit. Asiakirjoista tulee käydä ilmi käytetyt menetelmät ja saadut tulokset. Riskin arvioinnin asiakirjoista on käytävä ilmi muun muassa:

- koneen raja-arvot
- tehdyt oletukset (esimerkiksi käyttöiästä)
- tunnistetut vaaratekijät, vaaratilanteet ja vaaralliset tapahtumat
- mihin tietoihin riskin arviointi perustuu
- mitkä tavoitteet on tarkoitus saavuttaa turvallisuustoimenpiteillä
- valitut turvallisuustoimenpiteet
- jäännösriskit
- riskin arvioinnin lopputulos
- riskin arvioinnin kuluessa täytetyt lomakkeet [24].

Riskin arvioinnin asiakirjat ovat osa koneen teknistä dokumenttia, joka on koneasetuksen vaatima. Koneen turvallisuussuunnittelu on iteratiivinen prosessi, ja riskianalyysiin sekä riskien pienentämiseen joudutaan palamaan myöhemmässä suunnitteluvaiheessa. [23; 24.]

3.3 Turvallisuuteen liittyvät ohjausjärjestelmän osat

SFS-EN ISO 13849: Koneturvallisuus, turvallisuuteen liittyvät ohjausjärjestelmän osat [27] standardi on B-tyypin standardi. Standardia sovelletaan turvallisuuteen liittyvien ohjausjärjestelmien osien suunnitteluun ja riskin pienentämisen strategiaan. Standardissa esitellään myös suoritustasot (PL), luokat, turvatoiminnot ja turvallisuusvaatimukset. Osittain rinnakkaista standardia SFS-EN 62061 [2] sovelletaan sähköisen, elektronisen ja ohjelmoitavan elektronisen S/E/OE ohjausjärjestelmän suunnitteluun, koneeseen yhdistämiseen ja kelpuutukseen. Standardia SFS-EN 62061 käsitellään vain siltä osin, kun se soveltuu liikkuvien työkonien ohjausjärjestelmän oleellisiin komponentteihin tai osiin. Ohjausjärjestelmiä käsitellään erikseen koneasetuksen liitteen I luvussa 1.2. Ohjausjärjestelmästä erikseen mainitaan ohjauslaitteet, käynnistäminen, pysäyttäminen, tehonsyötön häiriöt sekä ohjaus ja toimintatapojen valinta.

Yleisesti ohjausjärjestelmien toiminnasta ja toimintavarmuudesta on määrätty seuraava:
”Ohjausjärjestelmät on suunniteltava ja rakennettava sellaisiksi, että ne estävät vaaratilanteiden syntymisen. Ennen kaikkea ne on suunniteltava ja rakennettava sellaisiksi, että:

- *ne kestävät tarkoitetut käyttörasitukset ja ulkoiset vaikutukset;*
- *ohjausjärjestelmän laitteisto- tai ohjelmistovika ei aiheuta vaaratilanteita;*
- *virheet ohjausjärjestelmän logiikassa eivät aiheuta vaaratilanteita; ja*
- *kohtuudella ennakoitavissa oleva inhimillinen erehdys käytön aikana ei aiheuta vaaratilanteita.*

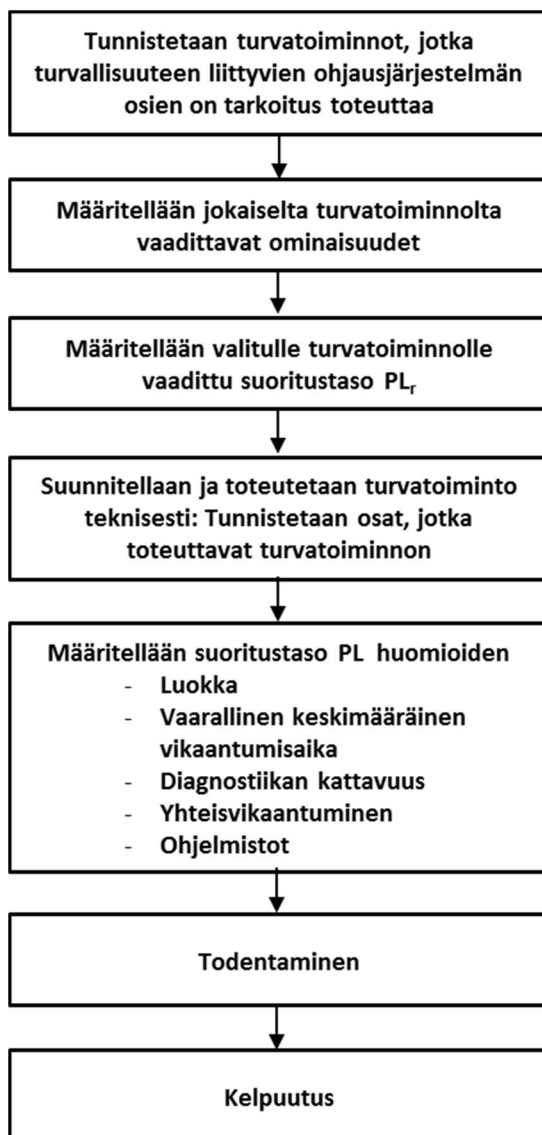
Erityistä huomiota on kiinnitettävä seuraaviin seikkoihin:

- *kone ei saa käynnistyä odottamattomasti;*
- *koneen ominaisarvot eivät saa muuttua hallitsemattomasti, jos tällainen muutos saattaa aiheuttaa vaaratilanteita;*
- *koneen pysähtymistä ei saa estää, jos pysäytyskäsky on jo annettu;*
- *mikään koneen liikkuva osa tai koneen kiinni pitämä kappale ei saa pudota tai sinkoutua;*
- *minkään liikkuvan osan automaattinen tai käsikäyttöinen pysäyttäminen ei saa estyä;*
- *turvallisuuden on pysyttävä täysin toimintakykyisinä tai annettava pysäytyskäsky; ja*
- *turvallisuuteen liittyviä ohjausjärjestelmän osia on käytettävä yhtenäisellä tavalla koneiden tai osittain valmiiden koneiden muodostamaan koko kokoonpanoon.”* [20, luku 1.2.1.]

Koneasetuksen vaatimukset ovat pääsääntöisesti yleisiä vaatimuksia, mutta langattomalle ohjaukselle on olemassa selkeä ja yksityiskohtainen vaade.

”Langattomassa ohjauksessa on aikaansaatava automaattinen pysäytys, jos oikeita ohjaussignaaleja ei saada tai jos yhteys menetetään.” [20, luku 1.2.1.]

Standardin 12100 mukaan tehdyn riskianalyysin myötä on löydetty koneen riskit ja päätetty millä menetelmillä riskejä voidaan poistaa tai pienentää. Jos riskin pienentämiseen liittyvän suojaustoimenpide riippuu ohjausjärjestelmästä, kutsutaan tätä ohjausjärjestelmän toimintoa tai sen osaa turvallisuuteen liittyväksi ohjausjärjestelmän osaksi. Kuvas-
 sa 11 kuvattu on turvallisuuteen liittyvien ohjausjärjestelmän osien iteratiivinen suunnitteluprosessi. Tämä prosessi yhdistetään riskin arvioinnin ja pienentämisen menetelmään (kuva 8), kun ohjausjärjestelmä on osa riskin pienentämistä.



Kuva 11 Turvallisuuteen liittyvien ohjausjärjestelmän osien iteratiivinen suunnittelu-prosessi [27]

Ohjausjärjestelmä koostuu monesta komponentista ja osajärjestelmästä. Turvallisuuteen liittyvä ohjausjärjestelmässä kaikkien komponenttien ja osajärjestelmien on toimittava oikein, tai vikaannuttava turvallisesti.

Ohjausjärjestelmän vaaratekijät ovat satunnaisia komponenttivikoja tai systemaattisia ohjelmistovirheitä. Systemaattiset virheet ovat suunnitteluvirheitä, jotka saavat ohjelmiston tai koneen toimimaan virheellisesti. Systemaattisten virheiden tyypillisyyden vuoksi ohjelmoitavalle logiikalle ja muille ohjelmoitaville ohjausjärjestelmille turvallisuusvaatimuksia suunniteltaessa ja arvioitaessa on otettava huomioon kaikki käyttöympäristön, koneen ja ohjausjärjestelmän turvallisuuteen vaikuttavat ominaisuudet. Systemaattisiin vikaantumisiin johtaa virheet turvallisuuden vaatimusten määrittelyssä, lait-

teiston suunnittelussa ja toteutuksessa, sekä ohjelmiston suunnittelussa ja toteutuksessa. [27; 28.]

Vaatimustenmäärittely on koko koneen elinkaaren ajan tapahtuvaa toimintaa. Vaatimukset vastaavat kysymykseen mitä pitää tehdä, kun taas suunnitelma kertoo miten vaatimus toteutetaan. Suurin osa turvallisuuskriittisistä virheistä tehdään vaatimustenmäärittelyvaiheessa [29]. Turvallisuusvaatimukset tulee kirjata ymmärrettävään muotoon. Ohjelmistojen turvallisuus pyritään varmistamaan todentamisella ja kelpuutuksella eli analyysillä. Todentaminen (*verification*) osoittaa, että järjestelmän syötteet tuottavat oikeita ja yhdenmukaisia tuloksia. Kelpuutus (*validation*) varmistaa, että turvallisuusvaatimukset toteutuvat. Monimutkainen ohjelmoitava ohjausjärjestelmä kelpuutetaan käyttämällä koko suunnitteluprosessin aikana useita erilaisia menetelmiä systemaattisten virheiden minimoimiseksi [28]. Ohjausjärjestelmän kelpuuttamista käsitellään laajemmin standardin SFS-EN ISO 13849 osassa 2 [30]. Turvatoiminnon suunnittelu on iteratiivinen prosessi ohjausjärjestelmän turvallisuuteen liittyvien osien suunnittelun sisällä:

vaatimukset – suunnittelu – todentaminen – kelpuutus –
uudet tarkemmat vaatimukset – suunnittelu – ...

Prosessin jäljitettävyys on tärkeää, kun kyseessä ovat turvallisuusvaatimukset. On pysyttävä osoittamaan, mikä suunnitelma toteuttaa turvallisuusvaatimuksen, millainen toimenpide on riskianalyysin avulla valittu ja kuinka se on todennettu. Turvallisuusvaatimusten lähteenä käytetään koneasetuksen ja standardien lisäksi

- riskianalyysia
- aikaisempia kokemuksia, esimerkiksi vahinkotilastoja
- asiakkaan, komponenttivalmistajan ja viranomaisen vaatimuksia
- suunnittelun ja testauksen tuottamia dokumentteja
- loppukäyttäjän palautetta.

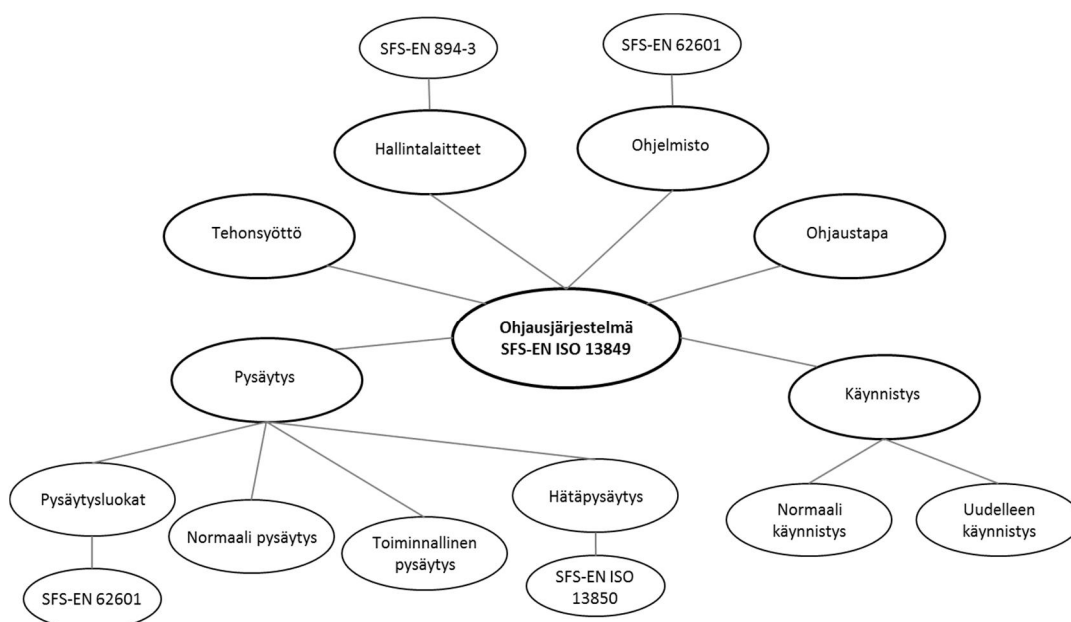
Riskianalyysi on osa todentamisprosessia. Jokaisella suunnittelun kierroksella tulee myös riskianalyysi tarkistaa ja tarkentaa. Riskianalyysissa syntyneet korjausehdotukset tulee dokumentoida ja niistä muodostuu uusia vaatimuksia. [29.]

Ohjausjärjestelmä ei saa aiheuttaa vaaratilanteita, vaikka virheitä tapahtuu. Virheitä yritetään välttää, ja toisaalta virheet yritetään löytää diagnostiikan avulla, jolloin virheisiin voidaan reagoida oikeilla tavoilla. Virheiden sietäminen kasvaa, kun ohjausjärjestelmä muodostuu rinnakkaisista järjestelmistä, jotka valvovat toisiaan ja jotka voivat paikata toistensa virheitä. Ohjelmiston lisäksi oikean tiedon prosessoimiseen liittyvät tiedonsiirtojärjestelmät, niin johdotetut kuin langattomatkin.

Turvatoiminnot ovat ohjausjärjestelmän toteuttamia turvallisuuteen liittyviä toimintoja ja niiden yksityiskohtia. Turvatoiminnot voivat olla vastauksia siihen, miten vaatimuk-

set toteutetaan. Turvatoiminto on toiminto, jonka vikaantuminen voi aiheuttaa välittömän riskin kasvamisen. Turvatoimintoja voivat olla pysäytystoiminto, odottamattoman käynnistymisen estäminen, kuittaustoiminto tai pakkotoiminto. Tehonsyöttö, siinä ilmenevät muutokset ja tehonsyötön menetys tai palaaminen ei saa aiheuttaa vaaratilanteita. Muutokset tehonsyötössä eivät saa aiheuttaa muutoksia koneen ominaisarvoissa tai käynnistää konetta odottamattomasti.

Tehonsyötön menetyksen jälkeen kone on saatettava turvalliseen tilaan, eikä koneen kannattelema taakka saa karata. Jo annetut pysähtymiskäskyt on saatettava loppuun tehonsyötöstä huolimatta. Kone voidaan pysäyttää normaalina pysäytyksenä, toiminnallisena pysäytyksenä tai hätäpysäytyksenä. Kuvassa 12 on jaoteltu ohjausjärjestelmän osia, ja niihin liittyviä standardeja, jotka voivat toteuttaa turvatoiminnon.



Kuva 12 Ohjausjärjestelmän osat ja toiminnot

Standardissa SFS-EN 62601 pysäytys jaetaan kolmeen luokkaan. Normaali pysäytys on luokassa 2. Kun vaikutetaan pysäytyksen tekevään hallintalaitteeseen, kone pysähtyy, mutta energiansyöttöä ei katkaista. Jos pysäytys tehdään turvallisuuteen liittyvänä pysäytyksenä, toiminnallisena pysäytyksenä, on pysähtyneenä olemista valvottava. Luokan 0 ja 1 pysäytyksissä energiansyöttö koneelle katkaistaan. Luokassa 0 energiansyöttö katkaistaan heti, ja luokassa 1 tehdään ensin vaadittavat hidastukset tai ohjaukset, ja vasta sen jälkeen katkaistaan energiansyöttö. Kummassakaan luokassa pysähtyminen ei saa aiheuttaa lisävaaraa.

Luokkia 0 ja 1 voidaan käyttää hätäpysäytyksenä. Hätäpysäytys ei ole varsinainen turvatoiminto vaan täydentävä suojaustoimenpide. Koneen on oltava tarpeeksi turvallinen ilman hätäpysäytystäkin. [2.] Hätäpysäytykselle on oma standardinsa SFS-EN ISO

13850. Kun kone pysäytetään hätäpysäytyksellä, on hätäpysäytys kuitattava käsikäyttöisesti. Kone ei saa käynnistyä uudelleen hätäpysäytyksen kuittauksen jälkeen, vaan vasta, kun käynnistämisen hoitavaan hallintalaitteeseen on vaikutettu. Riippumatta koneen pysäytystavasta uudelleenkäynnistämisen yhteydessä mikään kesken jäänyt toiminto ei saa jatkua yllättävästi. Jos sekä käynnistämisen että pysäyttämisen hallintalaitteisiin vaikutetaan samanaikaisesti, on pysähtymiskäskeytys aina ensisijainen.

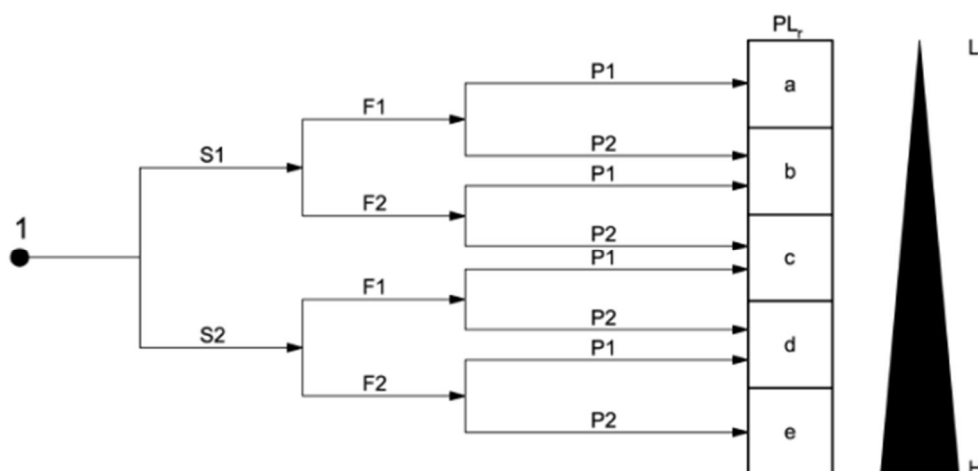
Ohjausjärjestelmä huolehtii koneen ohjauskäskeytyksistä ja toimilaitteiden liikuttamisesta. Ohjausjärjestelmä saa käskeytyksiä muista koneen osista tai käyttäjältä, ja reagoi niihin halutulla tavalla. Ohjausjärjestelmää käytetään myös koneen turvallisuuden toteutuksessa. Nämä kaksi ohjausjärjestelmän tehtävää tulee pitää erillään toisistaan. Vika ohjausjärjestelmässä ei saa vikaannuttaa turvallisuuteen liittyvän ohjausjärjestelmän osaa. Toiminnot ovat eriytettävä toisistaan niin ohjelmallisesti, kuin fyysisesti. [2; 27; 28.]

3.3.1 Suoritustaso ja turvallisuuden eheyden taso

Riskianalyysin tuottaman riskin vähentämisen tarpeen todentamisessa voidaan käyttää standardissa SFS-EN ISO 13849-1 esiteltyä suoritustasoa (PL). Suoritustaso määrittää ohjausjärjestelmän osien kykyä suorittaa turvatoiminto ennakoitavissa olevissa olosuhteissa. Suoritustaso valitaan sen mukaan miten hyvin ohjausjärjestelmä pystyy suorittamaan toivotun turvatoiminnon. Vaaditun suoritustason määrittelemine on riskin arvioinnin tulos, ja se on dokumentoitava jokaiselle turvallisuuteen liittyvälle ohjausjärjestelmän osalle. Suoritustaso vaikuttaa siihen riskin pienentämisen määrään, joka on tarkoitus toteuttaa. Suoritustasot a–e on jaettu niin, että a on matalin ja e vaativin taso. Kuva 13 on esitetty ohje vaaditun suoritustason PL_r määrittämiseksi riskin arvioinnin perusteella. Vaadittu suoritustaso määräytyy vaurion vakavuuden, vauralle altistumisen taajuuden kautta ja sen perusteella, onko vauron välttämine mahdollista. Suoritustason tilalla puhutaan myös turvallisuuden eheyden tasoista (SIL). Nämä termit käsittelevät samaa asiaa, mutta suoritustasoa käytetään standardissa SFS-EN ISO 13849-1, kun taas eheystasoista puhutaan standardissa SFS-EN 62061. [2; 27.]

Vaadittua suoritustasoa verrataan ohjausjärjestelmän suoritustasoon, joka arvioidaan seuraavien ohjausjärjestelmään ja sen komponentteihin liittyvien näkökulmien kautta:

- vaarallinen keskimääräinen vikaantumisaika ($MTTF_d$) jokaiselle yksittäiselle komponentille
- ohjausjärjestelmän luokat (B, 1, 2, 3 ja 4)
- diagnostiikan kattavuus (DC)
- yhteisvikaantuminen (CCF)
- turvatoiminnon käyttäytyminen vikatilanteessa
- turvallisuuteen liittyvä ohjelmisto
- systemaattisten vikojen hallinta ja niiden välttämine
- kyky toteuttaa turvatoiminto ennakoitavissa olevissa olosuhteissa. [29.]



Merkintöjen selitys

1 aloituskohta turvatoiminnon osuuden arvioimiseksi riskin pienentämisessä

L osuus riskin pienentämisessä pieni

H osuus riskin pienentämisessä suuri

PL_r vaadittava suoritustaso

Riskiiin liittyvät muuttujat

S vamman vakavuus

S₁ lievä (palautuva vamma)

S₂ vakava (palautumaton vamma)

F vaaralle altistumisen taajuus/kesto

F₁ harvoin, toisinaan ja/tai lyhyt altistumisaika

F₂ toistuvasti, jatkuvasti ja/tai pitkä altistumisaika

P mahdollisuus välttää vaara tai rajoittaa vahinkoa

P₁ mahdollista tietyissä olosuhteissa

P₂ tuskin mahdollista

Kuva 13 Vaadittavan suoritustason määrittäminen riskin arvioinnin avulla [27]

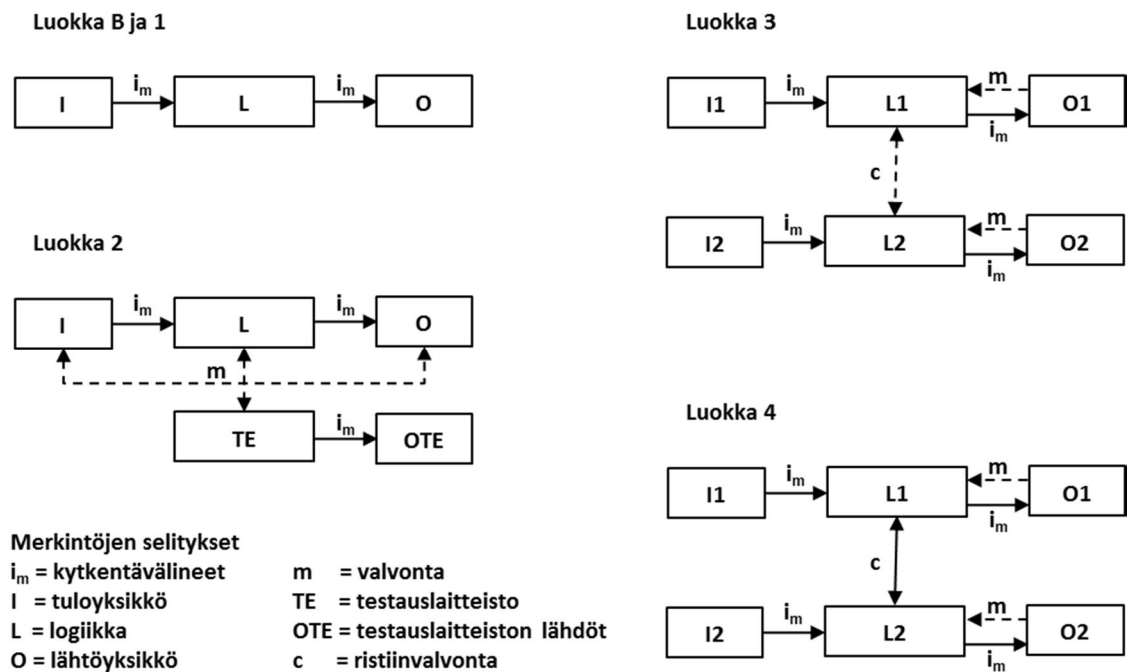
MTTF_d -arvo ilmoittaa komponentin keskimääräisen vaarallisen vikaantumisaian, ja se määritellään jokaiselle komponentille. Ensisijaisesti käytetään valmistajan ilmoittamaa MTTF_d -arvoa. Jos valmistaja ei ole ilmoittanut arvoa, standardin SFS-EN ISO 13849-1 liitteessä C on esitetty MTTF_d määrittämiseen käytettyjä keinoja. Viimeisenä vaihtoehtona, jos edellä mainituilla tavoilla ei ole saatu MTTF_d arvoa, käytetään keskimääräisenä vaarallisena vikaantumisaikana 10 vuotta. Käytettävän suoritustason määrittelemisen avuksi standardissa on määritelty viisi ohjausjärjestelmän luokkaa, jotka perustuvat määrättyihin käyttäytymistapoihin vikatilanteessa. Luokan valitsemiseen liittyy läheisesti diagnostiikan kattavuus, yhteisvikaantuminen ja käyttäytyminen vikatilanteessa. Luokka voidaan määrittää vikakestoisuuden ja diagnostiikan funktiona. Jotta diagnostiikan kattavuudella olisi merkitystä järjestelmän luotettavuudelle, on diagnostiikan katettava vähintään 60 % vioista. Luokissa 2-3 diagnostiikan on löydettävä lähes jokainen vika tai vikaantumistapa olisi otettava huomioon. [27; 28; 29.]

Taulukossa 3 on esitetty luokkien yksinkertaistetut vaatimukset.

Luokka	Perusvaatimus turvatoiminnolle	MTTF _d (vuotta)	Diagnostiikan kattavuus
B	Soveltuu ympäristö- ja käyttöolosuhteisiin	3 – 29	< 60 %
1	Hyvin koetellut komponentit ja turvallisuusperiaatteet	30 – 100	< 60 %
2	Ohjausjärjestelmä testaa toiminnon automaattisesti ajoittain, esim. käynnistyksen yhteydessä	3 – 100	60 – 98 %
3	Turvatoiminto täytyy pystyä toteuttamaan, vaikka ohjausjärjestelmässä on yksi vika	3 – 100	60 – 98 %
4	Turvatoiminto täytyy pystyä toteuttamaan, vaikka ohjausjärjestelmässä on yksi vika. Kaikkien vikojen on paljastuttava	30 – 100	99 – 100 %

Taulukko 3 Luokkien turvavaatimukset [28]

Standardin SFS-EN ISO 13849-1 liitteessä F on esitetty vaatimuksia ohjausjärjestelmän yhteisvioista. Yhteisviat ovat yksittäisestä tapahtumasta johtuvia eri kohteiden vikaantumisia kun ne eivät ole toistensa seurauksia. Luokissa B ja 1 yhteisvioilla ei ole merkitystä, koska jo yksi vika on vaarallinen. Näissä luokissa oletetaan, että ohjausjärjestelmän komponenteissa ei ole vikaa, tai jos vika esiintyy, niin vikaantuminen tapahtuu turvallisesti. Vika yleensä pysäyttää koneen. [29; 31.]



Kuva 14 Eri luokkien nimetyt rakenteet [29]

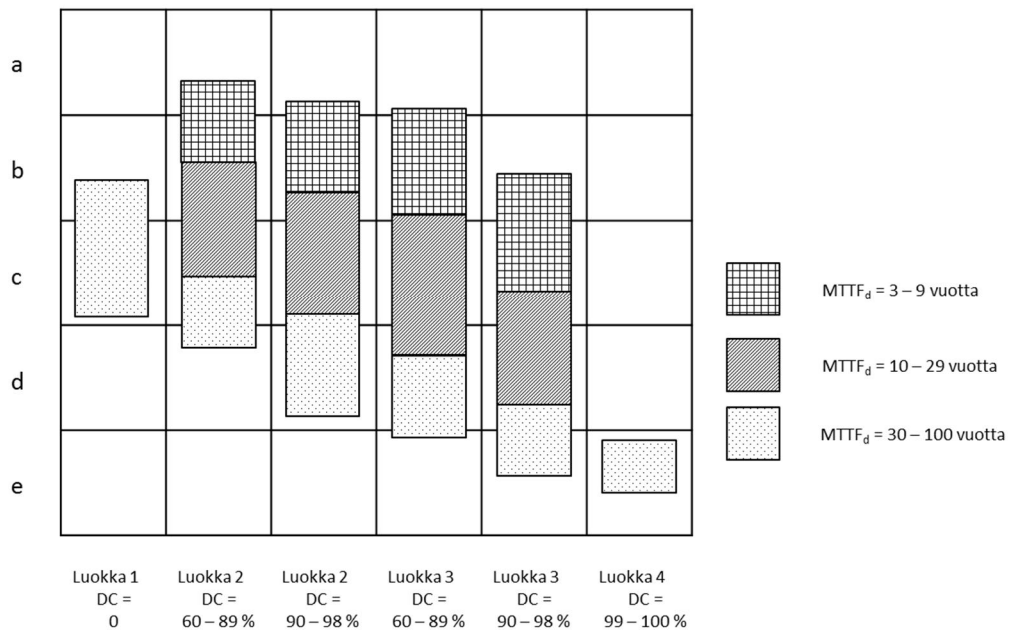
Luokissa 2 – 4 oletetaan, että alijärjestelmässä on vika. Turvallinen vikaantuminen mahdollistetaan valvonnalla ja kahdennuksilla. Ohjausjärjestelmän luokan valintaan liittyy myös ohjausjärjestelmän arkkitehtuuri (kuva 14).

Luokat B ja 1 ovat yksikanavaisia järjestelmiä, luokassa 2 on lisäksi testaus. Luokat 3 ja 4 ovat puolestaan kaksikanavaisia järjestelmiä. Koska ohjausjärjestelmät ovat monimutkaisempia kuin kuvatut arkkitehtuurit, on järjestelmä jaettava alijärjestelmiin. Jokaisen alijärjestelmän suoritustaso määritellään erikseen. [29.]

Turvallisuuteen liittyvän ohjausjärjestelmän osien luokkien ja diagnostiikan kattavuuden (DC) avulla nähdään kuvasta 15, mikä suoritustaso on mahdollista saavuttaa. Parempaan suoritustasoon pääsemiseksi voidaan parantaa joko diagnostiikan kattavuutta tai valita paremmin kestäviä komponentteja. Käytettävän suoritustason tulee olla samansuuruinen tai vaativampi kuin ohjausjärjestelmän vaadittava suoritustaso. Alijärjestelmät yhdistetään koskemaan koko ohjausjärjestelmää. Jos alijärjestelmissä on enemmän kuin kolme kappaletta alinta suoritustasoa, se laskee koko järjestelmän suoritustasoa yhdellä pykälällä. Keskimääräiset vaaralliset vikaantumiset yhdistetään alla olevalla kaavalla:

$$1/\text{MTTF}_{\text{dtot}} = 1/\text{MTTF}_{\text{d1}} + 1/\text{MTTF}_{\text{d1}} + \dots + 1/\text{MTTF}_{\text{dr}} \quad (3)$$

Suoritustaso



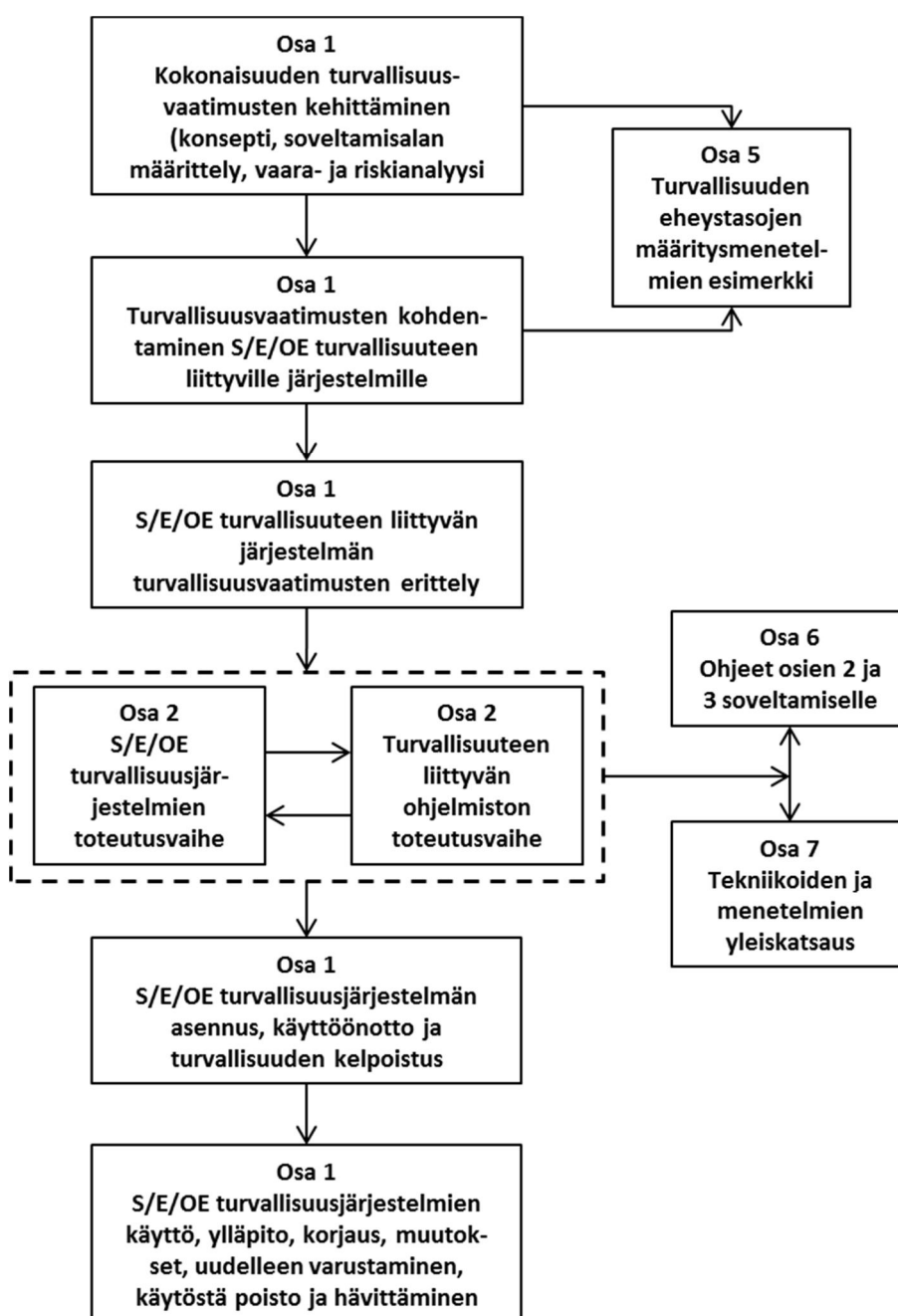
Kuva 15 Eri luokkien avulla saavutettava suoritustaso[28]

Luokkien sisällä paremmuus määräytyy diagnostiikan kattavuuden ja vikaantumisajan perusteella.

Turvallisuuteen liittyvien ohjausjärjestelmien osien määritetyt turvatoiminnot, saavutettu luokka ja suoritustaso on kelpuutettava standardin SFS-EN ISO 13849-2 mukaan, jotta voidaan varmistaa turvatoimintojen tukevan konekokonaisuuden turvallisuuden vaatimusmäärittelyä. [27.]

3.4 Toiminnallinen turvallisuus

Standardi SFS-EN 61508-1 [31] antaa yleisen ohjeistuksen tilanteihin, joissa elektroniikka, sähköisiä tai tietokonepohjaisia toimintoja käytetään toteuttamaan turvatoiminto.



Kuva 16 SFS-EN 61508 standardin rakenne [31]

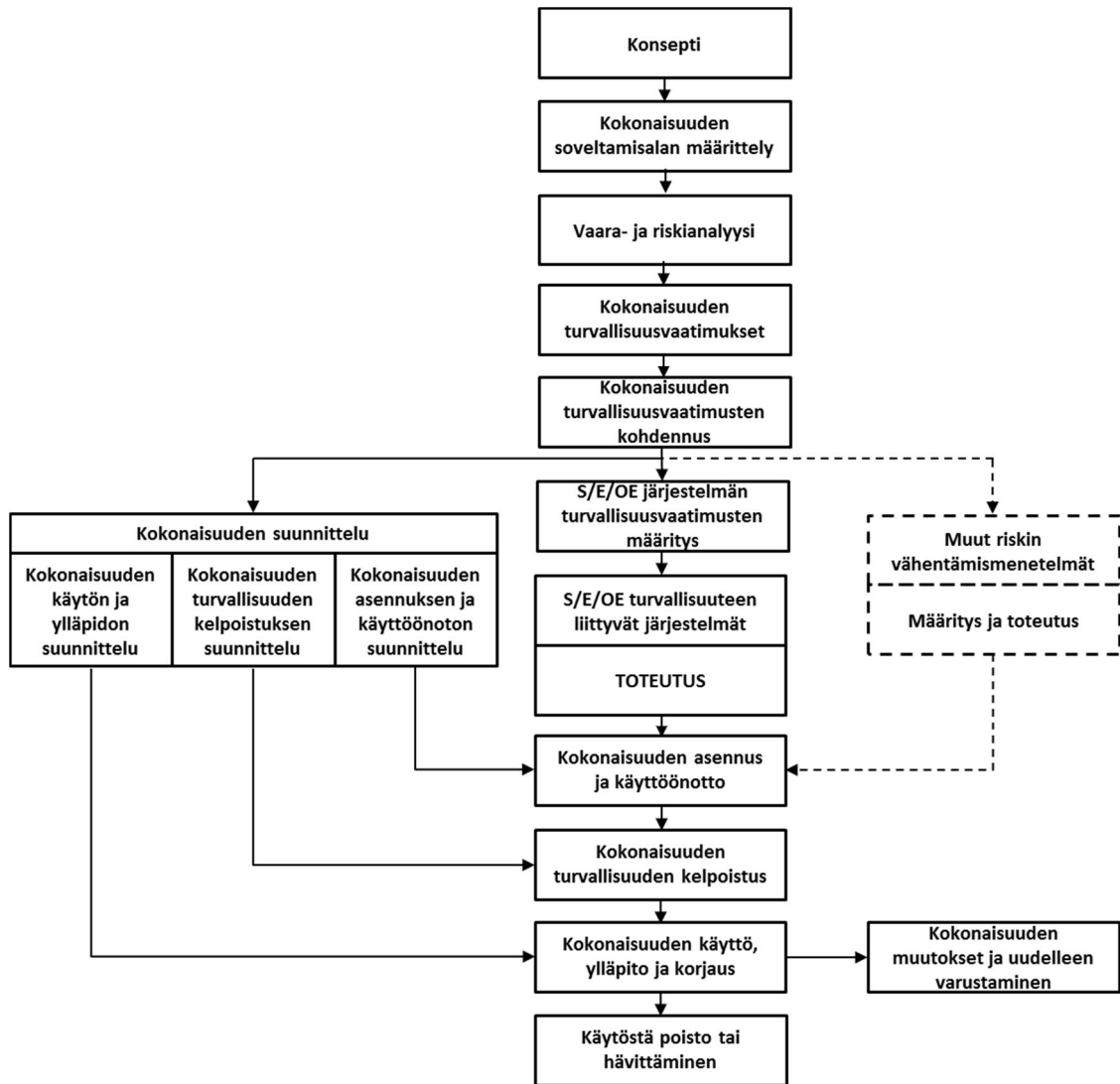
Standardiin SFS-EN 61508 kuuluu osan 1 lisäksi kuusi muuta osaa, jotka täydentävät yleisiä vaatimuksia. Kuvassa 16 on esitetty standardisarjan rakenne.

Toiminnallinen turvallisuus tarkoittaa sitä kokonaisturvallisuuden osaa, joka liittyy ohjattavaan laitteeseen ja sen ohjausjärjestelmään. Toiminnallinen turvallisuus on riippuvainen koneen eri järjestelmien kokonaisuuksien turvallisuudesta ja riskin pienentämismenetelmien oikeasta toiminnasta. Useimmissa tapauksissa turvallisuus saavutetaan useammalla järjestelmällä - mekaanisella, hydraulisella, sähköisellä, elektronisella tai ohjelmoitavalla elektronisella järjestelmällä. Turvallisuussuunnittelun tulee ottaa huomioon, ei vain yksittäisen järjestelmän komponentit, vaan turvallisuuteen liittyvien järjestelmien yhdistelmä. Tämä standardi käsittelee sähköisten, elektronisten ja tietokonepohjaisten järjestelmien toimintaa, mutta tarjoaa näkökulmia myös muihin teknologioihin. [31.]

S/E/OE turvallisuuteen liittyvien järjestelmien toteutus kätkee sisälleen ohjelmiston ja S/E/OE järjestelmän turvallisuuden elinkaaren. Nämä elinkaaret muodostuvat vaatimusten määrittelystä, suunnittelusta, kehityksestä, järjestelmän ohjelmiston ja laitteiden integroinnista, kelpoistussuunnitelmasta ja käytön ja ylläpidon menetelmistä. Standardi esittää kokonaisuuden, jossa käsitellään kaikkia turvallisuuden kannalta tärkeitä toimia, ja näiden vaateita, oikean turvallisuuden tason saavuttamiseksi.

Sähköisiä, elektronisia ja ohjelmoitavia elektronisia järjestelmiä on käytetty jo pitkään, ennen standardin 61508-1 julkaisua, suorittamaan turvatoimintoja. Standardin tarkoitus on antaa yleinen lähestymistapa turvatoimintoja suorittavien S/E/OE järjestelmiä käyttävien koneiden elinkaareen. Standardi yhdistää monet teknologiat, vaikka suoraanaisesti esittää vain turvallisuuteen liittyvät S/E/OE järjestelmät. Koneenrakennuksessa jokaiselle osajärjestelmälle - mekaaniselle, hydrauliselle, sähköiselle osajärjestelmälle ja ohjausjärjestelmälle - on omat standardinsa.

Toiminnallisen turvallisuuden standardi yhdistää nämä osajärjestelmät kokonaisuuksiksi, samoin kuin S/E/OE järjestelmä yhdistää koneen muut osajärjestelmät toimimaan yhdessä. Niinpä monet standardin käyttämistä termeistä ja määritelmistä on jo esitelty muissa standardeissa. Esimerkiksi suoritustaso, ja turvallisuuden eheyden tasot käsitellään esimerkein ja riskipohjaisen käsitteellisen rakenteen kautta, mutta standardi ei puutu minkään turvatoiminnon tason valintaan. [31.]



Kuva 17 Kokonaisuuden turvallisuuden elinkaari [31]

3.5 Hydraulinen tehonsiirto

Standardi SFS-EN ISO 4413 [32] on B-tyyppin standardi. Se korvaa standardit SFS-EN 982 ja 982 + A1, Hydraulisten ja pneumaattisten järjestelmien, sekä niiden komponenttien turvallisuusvaatimuksista. Standardi esittää vain ne hydraulikan erityisvaatimukset, joita ei ole standardissa SFS-EN ISO 12100 määritelty. Standardin SFS-EN ISO 4413 vaatimuksia voidaan muuttaa tai täydentää C-tyyppin konekohtaisissa standardeissa. Tämän standardin lisäksi on olemassa useita, esimerkiksi hydraulikkasyntereitä, letkuja ja putkia sekä paineakkuja koskevia standardeja.

Standardin SFS-EN ISO 4413 liitteessä A on merkittävien vaaratekijöiden luettelo, jonka mukaan hydraulijärjestelmän aiheuttamia vaaratilanteita voidaan käsitellä. Hydraulijärjestelmän turvallisuussuunnittelun lähtökohdaksi on hyvä ottaa perinteisen suunnittelutyön dokumentointi. Turvallisuussuunnittelu koetaan usein aikaa vieväksi ja hankalaksi. Hydraulijärjestelmän turvallisuusvaatimukset täydentävät hyvää suunnittelutyötä ja antavat tarvittavat tiedot sekä valmistajalle että käyttäjälle. Standardin SFS-EN ISO 4413 liitteessä B on esitetty hydraulisten järjestelmien ja komponenttien tietojenhankkimislomake, joka varmistaa yhdenmukaisuuden standardin kanssa.

Yleisiä suunnitteluperiaatteita ovat:

- järjestelmän käyttö- ja toimintavaatimukset on määriteltävä
- valitaan standardin mukaan valmistettuja komponentteja
- komponentit asennetaan niin, että ne sijaitsevat helppopääsyisessä paikassa
- komponentit asennetaan valmistajan suosittelimilla tavoilla
- komponenttien ja putkiston käyttöarvot eivät saa ylittää määritettyjä maksimiarvoja
- ensisijaisesti käytetään putkia, letkujen käyttö on perusteltu
- järjestelmässä käytettävistä nesteistä on tiedot helposti saatavissa
- materiaalien kestävyys ja soveltuvuus kyseiseen järjestelmään
- lämpötila, melu, vuodot tai tarkoittamattomat paineet eivät saa aiheuttaa vaaraa.

Yksittäisiä, huomioonotettavia asioita ovat:

- paineakun tiedot on merkittävä akkuun pysyvästi ja luettavasti
- ylipainetta vastaan suojaudutaan ensisijaisesti paineventtiilillä
- kaikkia komponentteja tai kokoonpanoja, joiden paino on yli 15 kg, on pystytävä nostamaan nostolaitteella. [32.]

Hydraulikomponentit ovat yleisesti hyvin koeteltuja komponentteja. Perinteiset venttiilit, vastavoimalla toimivat palloventtiilit, sylinterit ovat turvallisuuden kannalta luotettavia elementtejä. Sähköhydraulisiin komponentteihin tulee soveltaa sähköisten osien standardeja, tai sitten on ohjelmallisesti huolehdittava vikadiagnostiikasta ja turvallisesta vikaantumisesta esimerkiksi tehonsyötön häiriöiden aikaan.

Nykyään markkinoilla on yhä enemmän sähköhydraulisia turvakomponentteja. Ne on valmistettu standardien mukaan, ja niitä voidaan käyttää toiminnallisen turvallisuuden toteuttamiseksi tai komponentti itsessään on rakennettu toiminnallisen turvallisuuden toteuttajaksi. Komponenteissa on sisäänrakennettuna eri toimintojen mittaus, ja komponentit vikaantuvat turvallisesti sähköttömässä tilassa. Luotettavat komponenttivalmistajat ilmoittavat tuotteen täyttämät standardit ja niihin liittyviä yleisiä vaatimuksia. Komponenttien oikea käyttötarkoitus ja asentaminen järjestelmään ovat puolestaan koneenvalmistajan vastuulla.

4 LIKKUVAN TYÖKONEEN TURVALLISUUS-SUUNNITTELU

Koneasetuksen liitteen I kohdassa 3 on liikkuville työkoneille lisävaatimuksia yleisten vaatimusten lisäksi. Koneasetuksessa annetaan erityisiä määräyksiä

- työskentelypaikkaan
- ohjausjärjestelmään
- mekaanisilta vaaroilta suojautumiseen
- suojaamiseen muilta vaaroilta
- tietoihin ja merkintöihin [20].

Liikkuvista työkoneista on lisäksi useita EN-standardeja, joissa on kullekin koneelle erityisiä vaatimuksia. Ohjaamot, kulkutiet, suojaukset, jarrut ja hallintalaitteet noudattavat yhdenmukaistettuja ohjeistuksia. Yleisiä turvallisuusperiaatteita ovat:

- kulkutiet (SFS-EN ISO 14122)
- ergonomia (prEN 14386)
- hallintaelimet ja merkinantolaitteet (prEN 14386, SFS-EN 894)
- hätäpysäytys (SFS-EN ISO 13850)
- ohjaamo (SFS-EN ISO 3471, SFS-EN 15695)
- melu (SFS-EN ISO 4871, SFS-EN ISO 11688-1, SFS-EN ISO 11200)
- värinä (SFS-EN 1032 + A1)

Liikkuvista työkoneista on olemassa konekohtaisia C-tyypin standardeja, jotka voivat määritellä tiettyjä vaatimuksia yksityiskohtaisemmin. Koneasetus ei koske maatalous- ja metsätraktoreita, mutta näiden koneiden standardeissa on paljon huomionarvoisia kohtia, joita voi soveltaa muihin liikkuviin työkoneisiin. C-tyypin standardeja on:

- maansiirtokoneille (SFS-EN 474)
- liikkuville tienrakennuskoneille (SFS-EN 500)
- trukeille (SFS-EN 1726)
- maatalouskoneille (SFS-EN ISO 4254)
- traktoreille
- metsäkoneille.

Taulukossa 4 on eritelty joitain liikkuviin työkoneisiin ja niiden osajärjestelmiin liittyvistä vaatimuksista.

Ohjauspiiri	Vikaantuminen ei saa aiheuttaa ohjauksen menettämistä.
Ohjauslaitteet	On oltava kuljettajan käytettävissä ohjauspaikalta.
	Palautuvia kytkimiä tulee käyttää silloin kun ohjauskäskyn päälle jääminen voi aiheuttaa lisävaaraa.
	Pyöriin kohdistuvat äkilliset iskut eivät saa välittyä hallintalaitteille.
Elektroninen ohjauspiiri	Vaihteen odottamaton siirtyminen
	Koneen yllättävä liikkeelle lähtö, kun moottori on käynnissä ja vaihde vapaalla.
	Toimilaitteiden yllättävä liike
Käynnistyminen ja liikkuminen	Koneen on käynnistytävä ja liikuttava vain kuljettajan käytäessä hallintalaitteita.
	Ei saa lähteä liikkeelle käynnistettäessä.
	Jos koneessa on tukijalat tai muita tiettyyn liikkeeseen pakollisia suojaustoimenpiteitä, niin liikkeen on oltava riippuvainen siitä onko suojaustoimenpiteet käytössä.
	On oltava peruutushälytin
Pysähtyminen ja paikallaan pysyminen	Hätäpysäytys on toteutettava itsenäisellä ja helposti tavoitettavalla hallintalaitteella.
	Koneessa on oltava pysäköintijarru, jos turvallisuus vaatii paikallaan pysymistä.
Valaistus	On oltava liikkumiseen ja työhön tarvittava valaistus.
Vaaraa aiheuttavat osat	Kaikki kuumat osat ja voimansiirron liikkuvat osat on suunniteltava, rakennettava ja sijoitettava siten, että minimoidaan puristumisesta, leikkautumisesta, viilloista ja kosketuksesta aiheutuva riski.
Ohjaamo	On suojattava kuljettajaa iskuilta ja sinkoavilta osilta.
	On oltava lämmitetty
Hydrauliikka	Hydrauliikan letkun irtoamisesta ja iskeytymisestä sekä korkeapaineisen öljyn riskejä on pienennettävä kun paine on yli 5 MPa, lämpötila yli 50°, tai henkilö voi olla yhtä metriä lähempänä.
	Letkujen suojaaminen, kun ei voida käyttää putkia.
Muuta	Koneessa on oltava palosammutin.
	Akku on voitava kytkeä helposti irti koneen virtapiiristä.
	Hinaukselle on oltava asianmukaiset kiinnityspaikat.

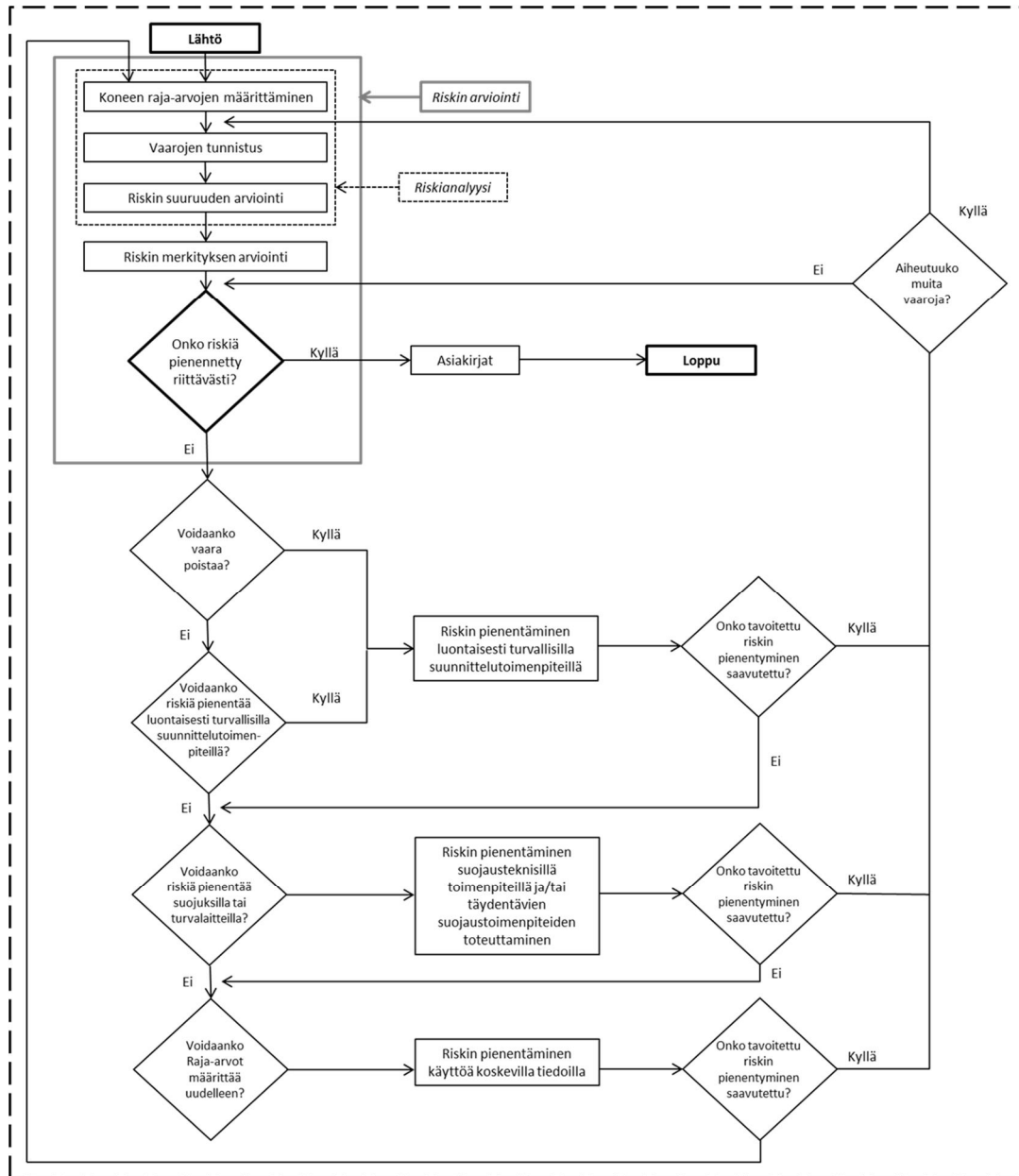
Taulukko 4 Liikkuvien työkoneiden erityiset turvallisuusvaatimukset [20; 21]

Yleisissä turvallisuusmääräyksissä koneen käyttäjäksi määritellään henkilö, joka asentaa, käyttää, säätää, huoltaa, puhdistaa, korjaa tai liikuttaa konetta. Liikkuvien työkoneiden suunnittelussa on tärkeää ottaa huomioon myös koneen kunnossapito- ja huoltohenkilöstö. Työtapaturman riski työkoneen vianetsinnässä ja korjauksen aikana on suuri. Työkone tulisi suunnitella niin, että huoltotoimenpiteet olisivat helppo suorittaa ympäristöstä riippumatta. Liikkuvien työkoneiden erityispiirre on, että vaaravyöhyke liikkuu työkoneen mukana. Yksi tavallisimmista liikkuvien työkoneiden aiheuttamista tapaturmista on koneen ulkopuolella olevalle henkilölle aiheutunut vahinko. Myös riskianalyysia tehtäessä on muistettava huoltohenkilöstö, ja koneen ympärillä olevat sivulliset henkilöt.

Turvallisuussuunnittelulla pyritään poistamaan vaara eli vamman tai terveyshaitan lähde. Vaaran täydellinen poistaminen onnistuu harvoin, jolloin suunnittelulla vähennetään seurauksia ja vaarallisen tapahtuman esiintymistä ja sille altistumista. Ne riskit, joita ei voida suunnittelulla, suojuksilla tai turvatoimenpiteillä poistaa, ovat jäännösriskejä. Jäännösriskit tulee dokumentoida ja merkitä koneeseen.

Turvallisuussuunnittelu on iteratiivinen prosessi, joka elää suunnittelun mukana. Liikkuvan työkoneen turvallisuussuunnittelun vaarana on prosessin hallitsematon laajeneminen. Jos liikkuvaan työkoneeseen ei ole C-tyyppin standardia, voi olla vaikeaa löytää se polku, jota turvallisuussuunnittelussa tulisi seurata. Vääränlainen riskianalyysin lähestymistapa saattaa johtaa siihen, että riskejä aliarvioidaan ja tuloksia muutellaan omin tarkoitusperien mukaan.

Kuvassa 18 on esitetty standardin SFS-EN ISO 12100 mukainen kaavio riskin pienentämisen prosessista, jota kappaleessa seurataan. Turvallisuussuunnittelussa tulisi huomioida, että monet arvot, suunnittelulähtökohdat ja dokumentit syntyvät teknisen suunnittelun kautta. Turvallisuuden huomioiminen suunnittelun yhtenä lähtökohtana helpottaa sekä liikkuvan työkoneen teknistä suunnittelua ja toteutusta, että turvallisuussuunnittelun dokumentointia.



Kuva 18 Standardin SFS-EN ISO 12100 mukainen riskin pienentämisprosessi [23]

4.1 Riskianalyysi

Riskianalyysi sisältää liikkuvan työkonteen raja-arvojen määrittämisen, vaarojen tunnistamisen ja riskin suuruuden arvioinnin. Riskianalyysi on osa riskin arviointia. Riskin arviointiin kuuluu riskianalyysin lisäksi riskin merkityksen arviointi ja johtaako riski toimenpiteisiin. Riskianalyysia varten tarvitaan liikkuvasta työkoneesta seuraavat tiedot:

- Koneen kuvaukseen liittyvät dokumentit:
 - käyttäjävaatimukset
 - koneen elinkaaren eri vaiheiden kuvaus
 - konepiirustukset / rakennepiirustukset
 - tarvittavat energialähteet
 - tarvittaessa samanlaisten koneiden dokumentaatiot
 - koneen käyttöä koskevat tiedot, jos saatavissa
- Säädöksiin, standardeihin ja muihin soveltuviin asiakirjoihin liittyvät tiedot:
 - sovellettavat säädökset
 - sovellettavat standardit
 - asiaankuuluvat tekniset vaatimukset
 - asiaankuuluvat, turvallisuuteen liittyvät ohjelehdet (data sheets)
- Käyttökokemuksiin liittyvät tiedot:
 - kyseiseen tai samankaltaiseen koneeseen kuuluvat tapaturmatiedot, epätavallisiin käyttötapauksiin liittyvät tiedot ja toimintahäiriötiedot
 - tietoja terveyshaitoista (päästöt, kemikaalit, melu, jne.)
 - kyseisen tai samankaltaisen koneen käyttäjäkokemukset
- Asiaankuuluvat ergonomiset periaatteet [23].

Liikkuvan työkonteen raja-arvojen määrittelyn tavoitteena on saada aikaan selkeä kuvaus koneesta ja sen ominaisuuksista. Raja-arvot tulee määrittellä kaikille liikkuvan työkonteen elinkaaren vaiheille. Raja-arvoista käy ilmi muun muassa:

- tehonsyöttö
- ohjaus
- toimintatavat
- liikkuminen
- koneen runko
- lisälaitteet
- nostoon ja hinaukseen liittyvät asiat [23].

Raja-arvoja määriteltäessä on huomioitava koneen erilaiset käyttäjät. Käyttäjäkuntaan luetaan myös ne henkilöt, jotka eivät käytä konetta, mutta altistuvat koneen vaaroille. Liikkuvien työkonneiden aiheuttamissa tapaturmissa sivullinen henkilö tai koneen ohjaamosta poistunut kuljettaja ovat usein niitä, joihin tapaturma kohdistuu.

Riskianalyysin tärkein osa on vaarojen tunnistaminen. Riskiä ei voida poistaa tai pienentää, jos vaaraa ei ole tunnistettu. C-tyypin standardeissa on käyty läpi tietyn kone-tyypin, esimerkiksi metsäkoneiden, pyöräkuormaajien ja trukkien vaarojen tunnistamista. Vaarojen tunnistaminen ja riskianalyysi eivät saa olla vain yhden menetelmän tai arvioijan varassa. Gauthier et al. [33] on tutkinut 31 eri riskien arviointimenetelmää 20 vaarallisen tilanteen kautta. Menetelmissä oli suuria eroja saman tilanteen arvioinnissa. Jottei vaaraa yli- tai aliarvioitaisi, tulisi pitävän lopputuloksen vuoksi käyttää useampaa eri menetelmää. [32.] Jokin menetelmä tai toimintatapa on valittava lähtökohdaksi tai muutoin prosessista voi tulla niin hajanainen, että osa vaaroista jää tunnistamatta, kun liikkuvaa työkonetta ei käydä järjestelmällisesti läpi. Missään tapauksessa tarkastuslistaa ei saa pitää ainoana oikeana dokumenttina. Vaarojen tunnistamisessa ei pidä hylätä luovaa ajattelua.

Taulukoon 5 on koottu standardeista 12100 ja 14121-2 esimerkki liikkuvan työkonteen vaaratekijöistä.

Vaaran tunnistaminen		
Tehtävä	Vaara	Mahdolliset seuraukset
Mekaaniset vaarat		
Koneella ajaminen	Kiihtyminen	Yliajetuksi tuleminen
Koneella työskenteleminen	Liikkuvan osan lähestyminen kiinteää osaa	Puristuminen
	Putoavat esineet	Isku
	Korkea paine	Injektoituminen
		Korkeapaineisen nesteen purkautuminen
	Epävakavuus	Kaatuminen
		Vakauden menetys
	Liike-energia	Puristuminen
	Liikkuvat osat	Isku
		Puristuminen
		Liikkuvien osien pysäytyksen vikaantuminen
Pyörivät osat	Leikkautuminen	
Vianetsintä, huoltotyöt	Varastoitunut energia	Isku
		Puristuminen
		Hallitsemattomat liikkeet
Sähköstä johtuvat vaarat		
Koneella ajaminen ja työskenteleminen Vianetsintä, huoltotyöt	Jännitteiset osat	Sähköisku
	Vikatilanteiden vuoksi jännitteiseksi tulleet osat	Sähköisku
		Vaarallinen liike
		Liikkuvien osien pysäytyksen vikaantuminen

Sähköstä johtuvat vaarat (jatkuu)		
	Oikosulku	Liikkuvien osien vikaantuminen
		Komponenttivauriot
		Sähköisku
		Tulipalo
Lämpötilasta johtuvat vaarat		
	Korkean lämpötilan omaavat kappaleet	Palovamma
		Tulipalo
Melusta johtuvat vaarat		
Koneella ajaminen ja työskenteleminen	Liikkuvat osat	Epämukavuus
	Kavitaatio	Tarkkaavaisuuden häiriöt
	Kuluneet osat	Stressi
	Epätasapainossa olevat pyörivät osat	Muutokset kuulossa
		Pysyvä kuulon menetys
Tärinästä johtuvat vaarat		
	Liikkuvien osien väärä kohdistus Kavitaatio Kuluneet osat	Epämukavuus
		Alaselän sairaudet
		Muut fyysiset sairaudet
Säteilystä johtuvat vaarat		
Materiaaleista tai aineista johtuvat vaarat		
Vianetsintä, huoltotyöt	Hydrauliöljy	Herkistyminen
		Ihovauriot
Ergonomiasta johtuvat vaarat		
Koneella työskenteleminen	Mittarien ja näyttöjen rakenne tai sijoittelu	Epämukavuus Stressi Tuki- ja liikuntaelinvaiat Väsymys Tarkkaavaisuushäiriöt
	Hallintalaitteiden sijoittelu	
Koneella työskenteleminen	Kohdevalaistus	
	Asento	
Huoltotyöt	Näkyvyys	
Huoltotyöt	Pääseminen	
Koneen käyttöympäristöön liittyvät vaarat		
Koneella työskenteleminen Huoltotyöt	Kosteus	Liukastuminen tai putoaminen
	Vesi	
	Öljy	
	Lika	Havaintovirheet
	Lämpötila	Epämukavuus Lievä sairaus
Vaarojen yhdistelmät		

Taulukko 5 Listaus vaaratekijöistä [23; 25]

Kun vaarat on tunnistettu, täytyy arvioida vaarasta aiheutuvan riskin suuruus. Riskin suuruuteen vaikuttaa, kuinka todennäköinen tapahtuma on ja mikä on seurauksen vakavuus.

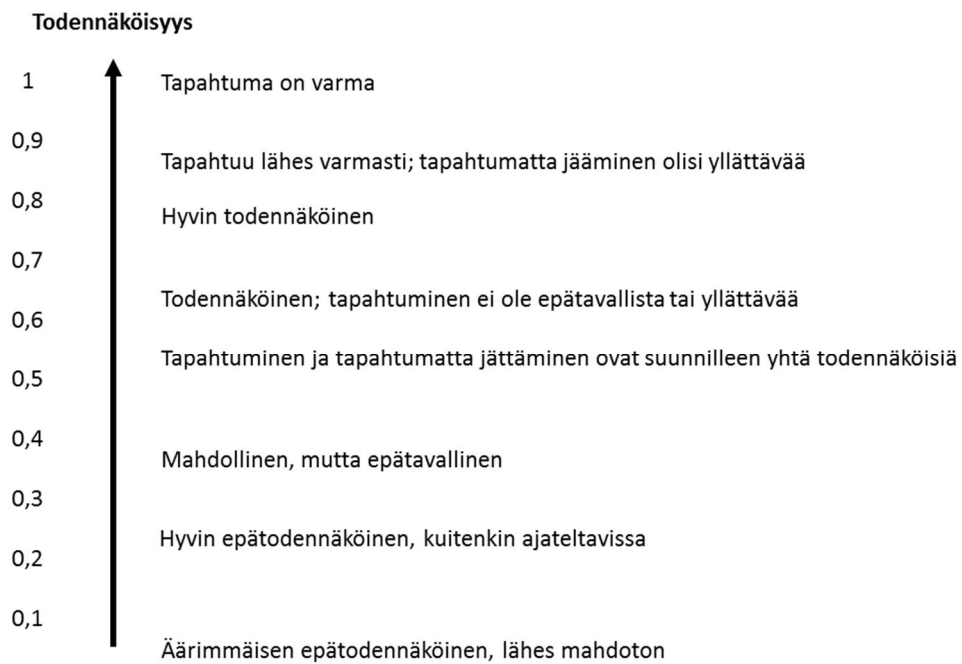
Riskin suuruuden arvioinnissa käytetään monesti kolmiportaista luokittelua, missä riski jaetaan kolmeen vakavuusasteeseen ja todennäköisyyteen. Haitan vakavuus voi olla lievä, vaikea tai suuri, ja haitan esiintymistodennäköisyys epätodennäköinen, mahdollinen tai todennäköinen. Siirilä [21] arvostelee menetelmää suppeudesta ja esittää vaihtoehtoisen useampiportaisen mallin. Vielä laajempi riskin arvioinnin malli on PILZ menetelmä. Menetelmässä tapahtuman todennäköisyydelle (LO) annetaan pistemäärä väliltä 0,33 – 15 ja tapahtuman vakavuudelle (DPH) 0,1 – 15. Todennäköisyyden ja vakavuuden lisäksi määritellään, kuinka usein vaarallinen tapahtuma esiintyy (FE), ja kuinka moni henkilö vaaralle altistuu (NP). Tapahtuman taajuus saa pistemäärät väliltä 0,5 – 5 ja altistuneiden henkilöiden määrä 1 – 12. Riskin lopullinen suuruus lasketaan kaavalla: [34.]

$$LO + DHP + FE + NP = \text{Riskin suuruus}$$

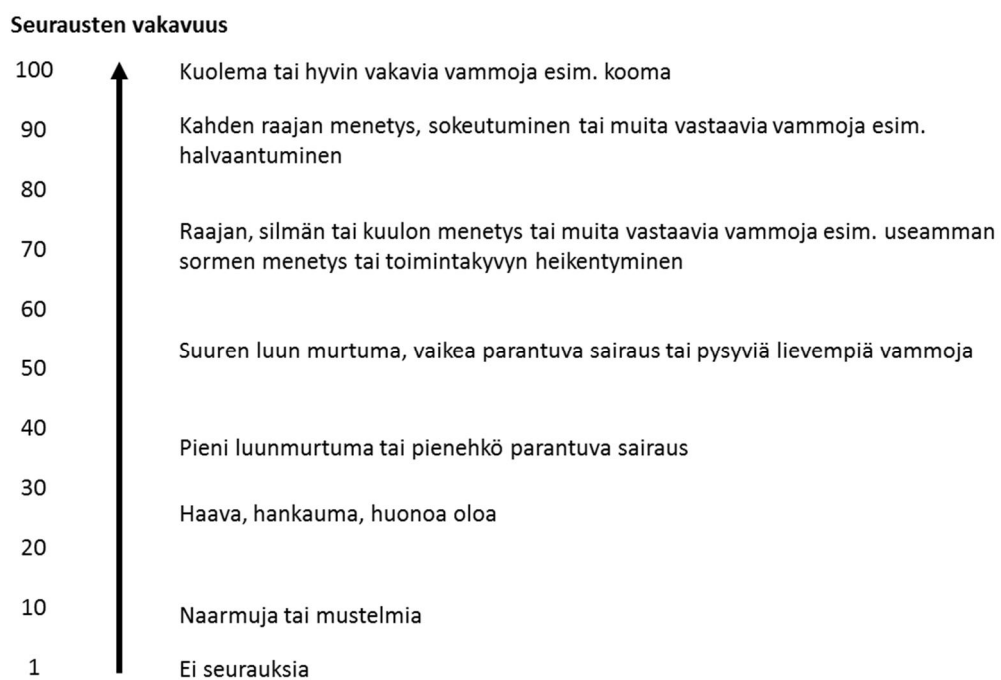
Liikkuvilla työkoneilla liian suppea riskin suuruuden arviointimalli voi johtaa siihen, että kaikkia riskejä tulee järjestelmän mukaan pienentää. Tällöin on mahdollista, että riskien arviointia tekevä työryhmä tai henkilö alkaa muokata riskianalyysia haluamaansa suuntaan. Vähäisiä vaaratilanteita jätetään tällöin täysin huomioimatta tai tämän prosessin seurauksena todellinen vaaratilanne jää näkemättä. Tässä luvussa käytetään tapahtumien todennäköisyyksien ja seurausten vakavuuksien jakamista isommalle vaihteluvälille Siirilän [21] mukaan. Tapahtumien todennäköisyyden luokittelu välille 0,1 – 1 on esitetty kuvassa 19 ja seurausten vakavuus asteikolla 1 – 100 kuvassa 20. Riskitaso saadaan kertomalla saadut lukuarvot keskenään. Riskitasot on määritelty toimenpiteiden mukaan viiteen luokkaan (taulukko 6).

Riskitaso		Tarvittavat toimenpiteet
Kuvaus	Lukuarvo	
Vähäinen	0,1 – 5	Ei tarvita toimenpiteitä
Siedettävä	6 – 15	Seuranta ja valvonta ja myöhemmin tehtävä uudelleen arviointi on tarpeen
Kohtalainen	16 – 28	Suunnittelua on jatkettava, riskiä saatava pienemmäksi. Käytössä olevalle koneelle korjaukset on tehtävä mahdollisimman pian.
Merkittävä	29 – 48	Suunnittelua on jatkettava, riskiä saatava pienemmäksi. Käytössä olevalle koneelle korjaukset on tehtävä heti.
Sietämätön	49 – 100	Suunnittelua on jatkettava, riskiä saatava pienemmäksi. Koneen käyttö tulee keskeyttää.

Taulukko 6 Riskitasot ja niiden toimenpiteet [21]



Kuva 19 Tarkasteltavien tapahtumien todennäköisyys [21]



Kuva 20 Tarkasteltavien tapahtumien seurausten vakavuus [21]

Riskianalyysia tehtäessä ohjausjärjestelmän turvallisuusmäärittelyyn tulee sisällyttää seuraavat asiat:

- turvallisuuden liittyvien ohjausjärjestelmien osien toteuttamat turvatoiminnot
- turvatoimintojen ominaisuudet
- turvallisuuden liittyvien ohjausjärjestelmien osien tarkat alku- ja loppukohdat
- ympäristöolosuhteet
- suoritustaso
- valitut luokat
- luotettavuuden kannalta merkittävät muuttuja (MTTF_d, DC)
- toimenpiteet systemaattisen vikaantumisen estämiseksi
- käytetyt teknologiat
- tarkastelussa mukana olleet turvallisuuden liittyvät viat
- vikojen poissulkemisen perustelut
- ohjelmistoa koskevat dokumentaatiot
- toimenpiteet kohtuudella ennakoitavissa olevista väärinkäytösten estämiseksi [27].

Ohjausjärjestelmän merkitys turvallisuudelle on sitä suurempi, mitä enemmän riskien vähennyksistä tehdään ohjausjärjestelmän toteuttaman turvatoiminnon kautta. Liikkuvissa työkoneissa ei voida käyttää kiinteitä suojuksia estämään henkilöiden pääsyä alueelle, tai pysäyttämään konetta vikatilanteissa. Ohjausjärjestelmän on pystyttävä takaamaan turvallisuus vikaantuessaankin. Turvallisuuden liittyvät ohjausjärjestelmän osat tulee toimia, vaikka jokin työkonetta liikuttavan ohjausjärjestelmän osa rikkoontuisi. Liikkuvan työkoneen ohjausjärjestelmän osille valitaan suoritustaso riskin suuruuden myötä. Mitä suurempi vastuu ohjausjärjestelmällä on liikkuvan työkoneen turvallisuudesta, ja mitä suuremmat riskit ovat kyseessä, sitä korkeampi suoritustaso on valittava. Taulukossa 7 on karkea jako mitä suoritustasoa (PL) tai eheystasoa (SIL) pitää käyttää millekin riskitasolle. [28.]

Riski \	Vähäinen	Siedettävä	Kohtalainen	Merkittävä	Sietämätön
Suoritustaso	a	b	c	d	e
Eheystaso	-	1	1	2	3

Taulukko 7 Suoritustason tai turvallisuuden eheystason valitseminen tietyn suuruiselle riskille [28]

Suoritustaso saadaan valittua ohjausjärjestelmän luokkien ja luotettavuuden kannalta merkittävien muuttujien kautta. Ohjausjärjestelmän systemaattisen vikaantumisen estämiseksi ohjausjärjestelmää tulee testata. Ohjelmiston turvallisuusvaatimusten mukaisuus varmistetaan todentamisella ja kelpuutuksella.

Riskien arviointi ja riskianalyysi kuuluvat osana tekniseen rakennetiedostoon. Riskien arvioinnin dokumentoinnin vähimmäisvaatimukset esitetään SFS-EN ISO 14121 standardissa. Riskin arviointi ei ole vain tuotekehitys- tai suunnittelutyön alussa tehtävä työvaihe, vaan riskien arviointia tehdään koko liikkuvan työkonteen elinkaaren ajan, kun koneesta saatava tieto tarkentuu tai muuttuu.

4.2 Riskien pienentäminen

Riskianalyysissa esiin tulleet riskitekijät on ensisijaisesti poistettava luontaisilla suunnittelutoimenpiteillä. Kaikkia riskejä ei kuitenkaan voida poistaa, jolloin riskejä pienennetään suojausteknisillä toimenpiteillä tai täydentävillä suojaustoimenpiteillä. Liikkuvissa työkoneteissa riskien pienentäminen on haastavaa työkonteen liikkumisen ja työtehtävien vuoksi. Osaa riskeistä voidaan pienentää luontaisesti turvallisilla toimenpiteillä. Liikkuvissa työkoneteissa voidaan käyttää hyväksi havaittuja komponentteja ja ohjaamo suunnitellaan ergonomia- ja kestävyysvaatimusten mukaan. Usein liikkuvan työkonteen käyttöominaisuuksien vuoksi sen ympäristöä ei voida aidata tai estää henkilöiden oleskelua liikkuvan työkonteen läheisyydessä.

Vaara-alue kulkee liikkuvan työkonteen mukana. Koska työkonteen fyysinen koko on rajoitettu, ja tiettyjä liikkuvalla työkoneteelle olennaisia toimintoja ei voida rajoittaa, suojaus ei pystytä jokaiseen vaaralliseen paikkaan asentamaan. Tällöin ohjausjärjestelmän osuus riskien pienentämisessä kasvaa. Turvallisuuteen liittyvän ohjausjärjestelmän tehtävänä anturitiedon, ohjelmakäskyn tai muun havainnon pohjalta on:

- pysäyttää liikkuva työkone turvallisesti
- pysäyttää kone nopeasti hätätilanteessa
- pitää kone pysäytettynä niin kauan, kun vaaratilanne vallitsee (estää odottamaton käynnistys)
- pitää koneen nopeus tai teho alennetulla tasolla vaarallisen tilanteen aikana
- estää koneen osan tai työlaitteen rikkoutuminen
- sallia tietty toiminta vaaratilanteen aikana vain pakkoajolla
- mahdollistaa puristuksiin tai muuten loukkuun jääneen henkilön vapauttaminen.

Jäännösriskkejä jää liikkuvaan työkoneteeseen aina. Näitä yritetään vähentää kuljettajien koulutuksella ja vaaroista varoittamalla.

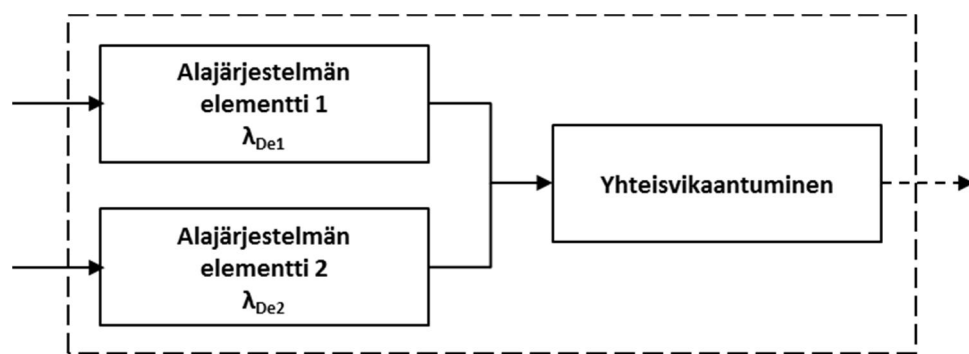
Liikkuvat työkoneteet ovat pääsääntöisesti massaltaan ja voimaltaan sellaisia, että tapaturmat voivat johtaa kuolemaan tai muuhun vakavaan tapaturmaan. Liikkuvissa työkoneteissa vaarallisia alueita tai toimintoja on lähes mahdotonta suojata suojuksin ilman, että työkoneteen tarkoitettu toiminto estyy. Riskien pienentäminen ja turvallisuus vikaantumisesta huolimatta tehdään liikkuvan työkoneteen ohjausjärjestelmien luokkien avulla,

ja turvallisuuden varmistamisella vikatilanteessa. Ohjausjärjestelmän luokkia saadaan nostettua diagnostiikkaa laajentamalla, komponenttien vikasietoisuutta parantamalla ja yhteisvikaantumista välttämällä.

Ohjausjärjestelmä on monimutkainen järjestelmä, ja se tulee jakaa pienempiin osiin, kun tarkastellaan ohjausjärjestelmän turvallisuutta. Alajärjestelmät koostuvat elementeistä, mikä voi olla yksittäinen komponentti tai komponenttiryhmä. Alajärjestelmien arkkitehtuurit esiteltiin luvussa 3.3.1. Jos yksinkertainen alajärjestelmä on suunniteltu ja kelpuutettu standardien mukaan, niin luokan valinnassa voidaan käyttää vaarallisen vikaantumisen todennäköisyyden kynnsarvoa PFH_D . Kynnsarvo on funktio alajärjestelmän keskimääräisestä vikaantumisajasta MTTF, testauksen ja tarkistuksen aikavälistä T , ja diagnostiikan kattavuudesta DC . Yksinkertainen tapa, alajärjestelmien vaarallisten laitevikaantumisien kynnsarvon laskemiseen, on esitelty standardissa SFS-EN 62061.

Kynnsarvon funktioon vaikuttaa alajärjestelmän perusrakenne. Kun alajärjestelmän vikasietoisuus on nolla, niin elementin vikaantuminen aiheuttaa myös turvallisuuteen liittyvän ohjausjärjestelmän vikaantumisen. Vikasietoisuuden ollessa yksi, minkä tahansa elementin vikaantuminen yksistään ei aiheuta turvallisuuteen liittyvän ohjaustoiminnon menettämistä. Diagnostiikkatoiminnolla saadaan käynnistettyä vikaan reagoiva toiminto. Mitä kattavampia diagnostiikkatoiminnot ovat, sitä pienempi on vaarallisten vikaantumisten todennäköisyys.

Tarkastellaan lähemmin alajärjestelmää, jonka vikasietoisuus on yksi (kuva 18) ja mitä diagnostiikka merkitsee alajärjestelmässä (kuva 21). [2.]



Kuva 21 Alajärjestelmä vikasietoisuus yksi ilman diagnostiikkaa [2]

Alajärjestelmän vaarallisen vikaantumisen todennäköisyys on

$$\lambda_{Dss} = (1 - \beta)^2 * \lambda_{De1} * \lambda_{De2} * T_1 + \beta * (\lambda_{De1} + \lambda_{De2})/2 \quad (4)$$

Kaavassa käytetyt merkit ovat:

Alajärjestelmän elementin vikataajuus $\lambda = 1/MTTF$

Alajärjestelmän elementin vaarallisen vikaantumisen taajuus = λ_{De}

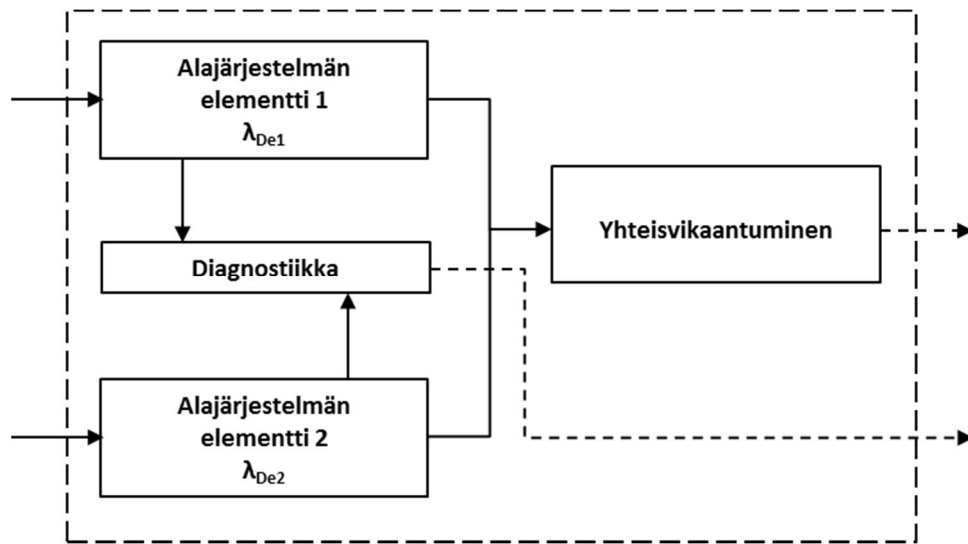
Yhteisvikaantumisalttius β

Määräaikaistestausten aikaväli tai elinkaaren pituus, riippuen siitä kumpi on pienempi T_1

Tästä todennäköisyydestä saadaan vaarallisen vikaantumisen todennäköisyyden kyn-
nysarvo

$$PFH_{DSS} = \lambda_{DSS} * 1h \quad (5)$$

Diagnostiikan lisääminen alajärjestelmään vähentää vaarallisen vikaantumisen vikataa-
juutta. Kuvassa 22 on kuvattu yllä olevaa alajärjestelmää diagnostiikan lisäämisen jäl-
keen.



Kuva 22 Alajärjestelmä vikasietoisuus yksi ja diagnostiikka [2]

Alajärjestelmän vaarallisen vikaantumisen todennäköisyys saadaan nyt

$$\lambda_{DSS} = (1 - \beta)^2 * \{ [\lambda_{De1} * \lambda_{De2} * (DC_1 + DC_2)] * T_2/2 + [\lambda_{De1} * \lambda_{De2} * (2 - DC_1 - DC_2)] * T_1/2 \} + \beta * (\lambda_{De1} + \lambda_{De2})/2 \quad (6)$$

Kaavassa on käytetty merkintöjä:

Alajärjestelmien diagnostiikan kattavuus DC

Diagnostiikkatestauksen aikaväli T_2

Määräaikaistarkastuksen aikaväli tai elinkaaren pituus T_1

Diagnostiikkatoiminto toteutetaan jokaiselle alajärjestelmälle. Diagnostiikkatoiminto voidaan toteuttaa:

- samalla alajärjestelmällä, johon diagnostiikkaa tarvitaan
- ohjausjärjestelmän muilla turvallisuuteen liittyvillä alajärjestelmillä

- ohjausjärjestelmän alajärjestelmällä, joka ei suorita turvallisuuteen liittyvää toimintaa.

Diagnostiikkatoiminnon on täytettävä vaatimukset systemaattisten vikojen välttämiseksi ja hallitsemiseksi. Diagnostiikkatoimintojen vikaantuminen itsessään on otettava huomioon. [2.] Diagnostiikan kattavuudesta ja yhteisvikojen arvioinnista löytyy lukuarvot ja tarkemmat taulukot standardin SFS-EN ISO 13849-1 liitteistä E ja F, sekä tämän kappaleen taulukosta 8.

Yhteisvikaantuminen on tilanne jossa kaksi tai useampi alijärjestelmä, tai yhden alijärjestelmän molemmat kanavat, vikaantuvat samanaikaisesti jonkin tapahtuman seurauksesta, ja johtaa jonkin turvallisuuteen liittyvän ohjaustoiminnon menettämiseen. Yhteisvikojen arviointiin on standardissa SFS-EN 62061 laskentamenetelmä. Yhteisvikaantumisen pisteytys, todennäköisyyden laskemiseksi, on taulukossa 8. Yhteisvikaantumisen syy voi olla suunnittelussa, käytössä tai kunnossapidossa tapahtunut virhe. Yhteisvikaantumisen syitä voivat olla esimerkiksi:

- yhteisten laitteistojen käyttäminen
- toiminnallinen riippuvuus alijärjestelmien kesken
- fyysisen tekijöiden vaikutus, esimerkiksi johdon katkeaminen tai irtoaminen
- komponenttien fyysinen läheisyys, jolloin sama ulkopuolinen toiminto rikkoo molemmat komponentit.
- ohjelmiston virheet.

Yhteisvikoja voi välttää eriyttämällä komponentteja toisistaan tai tehonlähteistä, ja kahdentamalla komponentteja tai tekniikoita. Yhteisvirheet voidaan löytää testauksen avulla. Pelkkä yksikkötestaus ei tässä tapauksessa riitä, vaan ohjausjärjestelmän on oltava liitettynä koko liikkuvan työkoneen järjestelmään. Kaikkia tapauksia ei suunnitellulla koneella voi turvallisesti testata, tai vikojen luominen järjestelmään ei onnistu. Reaaliaikaisilla simulointimalleilla on mahdollista testata koko järjestelmää ja yksittäisen vian vaikutusta turvallisesti ja tarkasti. Turvakriittisen ohjausjärjestelmän testausta simulointimallilla käsitellään luvussa 5.

Kohde	Pisteet
Erillisuus tai erottelu	
Ovatko turvallisuuteen liittyvän sähköisen ohjausjärjestelmän yksittäisten kanavien signaalikaapelit reititetty erillisesti muista kanavista kaikissa kohdissa tai ovatko ne riittävästi suojattu?	5
Jos käytetään tietojen koodausta ja purkua, onko se riittävä signaalien siirtovirheiden paljastumiseksi?	10
Ovatko turvallisuuteen liittyvän sähköisen ohjausjärjestelmän signaalikaapelit ja energiansyöttökaapelit erotettu kaikissa kohdissa tai ovatko ne riittävästi suojattu?	5
Jos alajärjestelmän elementit voivat osaltaan vaikuttaa yhteisvikaantumiseen, ovatko ne järjestetty fyysisesti erotettuihin laitteisiin omissa paikallisissa suojakoteloissaan?	5
Erilaisuus ja varmennus	
Käytetäänkö alajärjestelmässä erilaisia sähköisiä teknologioita, esimerkiksi yhtenä elektroninen tai ohjelmoitava elektroninen rele ja toisena sähkömekaaninen rele?	8
Onko alajärjestelmässä käytetty elementtejä, joissa käytetään erilaisia fysikaalisia periaatteita (esimerkiksi suojuksen oven asennon tunnistavat elementit, joissa käytetään mekaanisia ja magneettisia tunnistustekniikoita)?	10
Käytetäänkö alajärjestelmissä hyväksi elementtejä, joissa on eriaikaisuutta toimintojen suorittamisessa tai vikamuodoissa?	10
Onko alajärjestelmän elementeillä diagnostiikkatestausta aikavälillä, joka on enintään yksi minuutti?	10
Monimutkaisuus, rakenne ja sovellus	
Onko alajärjestelmien kanavien ristiinkytkentä estetty lukuun ottamatta tilannetta, jossa sitä on tarkoitus käyttää diagnostiikkatestaukseen?	2
Arviointi ja analysointi	
Onko vika- ja vaikutusanalyysin tulokset tutkittu yhteisvikaantumisten lähteiden määrittämiseksi ja onko etukäteen määritetyt yhteisvikaantumisten lähteet poistettu suunnittelun avulla?	9
Onko kenttälaitteiden vikaantumiset analysoitu ja tulokset otettu huomioon suunnittelussa?	9
Ammattitaito ja koulutus	
Ymmärtävätkö alajärjestelmän suunnittelijat yhteisvikaantumisten syyt ja seuraukset?	4
Ympäristöolosuhteiden hallinta	
Ovatko alajärjestelmän elementit soveltuvia toimimaan kaikissa tilanteissa niissä lämpötilan, kosteuden, korroosion, pölyjen, värinän jne. rajoissa, joihin ne on testattu käyttämättä ulkoisten ympäristöolosuhteiden hallintaa?	9
Onko alajärjestelmien sähkömagneettisten häiriöiden sieto liitteessä E esitettävien vaihteluvälien ja niiden rajojen mukainen?	9

Taulukko 8 Yhteisvikojen pisteytys [2; 21]

4.3 Todentaminen ja kelpuutus

Toiminnallisen turvallisuuden ylttäminen vaaditulle tasolle varmistetaan todentamisella (verification) ja kelpuutuksella (validation). Todentaminen ja kelpuutus tapahtuvat lähinnä erilaisten testien kautta, mutta simulointia ja erilaisia analyyseja voidaan käyttää yhtälailla. Todentamisella ja kelpuutuksella tarkistetaan, että turvallisuusvaatimukset täytetään ja ne ovat oikeellisia. Tämän tekevät henkilöt, jotka ovat riippumattomia järjestelmän suunnittelusta ja toteutuksesta.

Standardissa SFS-EN ISO 13849-2 [30] esitetään turvallisuuteen liittyvien ohjausjärjestelmien osien ja luokkien sekä suoritustasojen kelpuutusprosessi. Standardin liitteessä C on opastava hydraulisten järjestelmien kelpuutustyökalu. Tämä liite on otettava huomioon, kun hydraulisia järjestelmiä käytetään yhdessä muiden teknologioiden kanssa turvatoimintona, ja turvakriittisiä hydraulisia komponentteja yhdistetään tai ohjataan sähköisesti. Ohjausjärjestelmän ohjelmistojen kelpuutusta käsitellään lisäksi standardissa SFS-EN 61508-3. Kelpuutus voidaan saavuttaa analyysien ja testausten yhdistelmällä. Standardeissa määritellään ne olosuhteet, joissa testaus voidaan suorittaa. Kelpuutusprosessi olettaa, että suoritustaso (PL) on arvioitu standardin SFS-EN ISO 13849-1 mukaan.

4.3.1 Hydrauliikka

Energiattomaksi tekemiseen sovelletaan standardissa SFS-EN ISO 12100 esiteltyä mekanismin käynnistämistä tai pysäyttämistä. Liikkuvan työkoneen jarrujärjestelmä on kahdennettava niin että pääjarrujärjestelmän vikaantuessa hidastaminen ja pysäyttäminen voidaan toteuttaa varajärjestelmällä. Hydraulisen paineen menetys ei saa aiheuttaa lisävaaraa. Hydraulijärjestelmässä tulee olla paineen ja nopeuden rajoittamiseen omat venttiilit ja varastoitunut energia pitää pystyä purkamaan tarvittaessa. Hyvin koeteltuja turvallisuusperiaatteita ovat:

- Hydraulinesteen tilan valvonta oikein valituilla suodattimilla ja suodattimen tukkeutumisen ilmaisimella.
- Turvakriittisen pysäytystoiminnon suorittavalla venttiilillä on positiivinen peitto.
- Ohjausluistin siirtäminen turvalliseen asemaan suuremmalla kytkentävoimalla, esimerkiksi pinta-alasuhteen avulla.
- Kuormituspaineella suljettava venttiili
- Liikkuvan osan turvallinen asema pidetään mekaanisesti paikoillaan, pelkkä kitka ei riitä.

Hyvin koetelluista hydrauliikkakomponentteja ei ole standardissa eritelty. Komponentit ovat sovelluskohtaisia ja pääsääntöisesti hyvin koeteltuja, jos ne ovat yhdenmukaistettujen standardien mukaan valmistettuja. [30.]

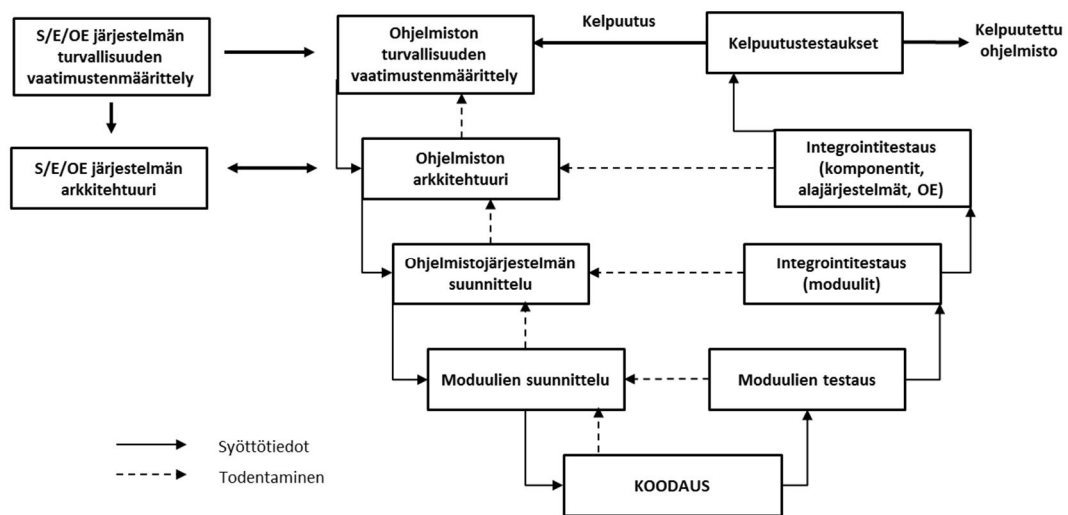
Vikojen poissulkemista käsitellään suuntaventtiilin, sulku-, vasta- ja vaihtovastaventtiilien, virtaventtiilien, paineventtiilien, metalliputkistojen, letkujen ja liittimien, suodattimien, energian varastoinnin ja anturien osalta. Anturien vikaantumista ei voida sulkea pois, vaan se täytyy ottaa huomioon järjestelmää suunniteltaessa ja koko elinkaaren ajalta. Energian varastoinnin kohdalla viat voidaan sulkea pois oikeilla komponenttivalinnoilla, lukuun ottamatta kaasun ja hydraulinesteen välissä olevan erotusosan vuotoa. Oikeat komponenttivalinnat johtavat vikojen poissulkemiseen myös suodattimien kohdalla. Suodattimen antureita ja venttiilejä koskevat samat säännöt kuin antureita ja venttiileitä yleensä. Letkujen ja liittimien tukkeutuminen voidaan sulkea pois oikealla nimelishalkaisijalla. Vuotoa ei voida jättää huomioimatta, vaan sen aiheuttamat riskitekijät on otettava huomioon muilla keinoin. Metalliputkistoa käytettäessä mitoituksella ja materiaalivalinnalla voidaan sulkea pois niin tukkeutuminen, murtuminen, vuoto kuin liittimien vikaantumisetkin. [30.]

Venttiileissä rakenteen rikkoutuminen voidaan sulkea pois jos rakenne, mitoitus ja asennus on tehty tarkoituksenmukaisesti. Suunta- ja paineventtiileissä vuodon aiheuttamia vikoja ei tarvitse huomioida, jos käytetään istukkaventtiiliä ja riittävää suodatusjärjestelmää. Pitkän käyttöajan kuluessa syntyvää muutosta vuodon tilavuusvirrassa ei voida sulkea pois, vaan siihen on kiinnitettävä huomiota kaikkien venttiilien kohdalla käyttöön määrittämisessä ja huoltoväleissä. Suuntaventtiileissä kytkentäaikojen muutoksien tuomista riskeistä päästään, jos käytetään erityisentyypistä patruunamallista istukkaventtiiliä. Sulku-, vasta- ja vaihtovastaventtiileissä kytkentäaikojen muutosta ei voida sulkea pois. [30.]

Venttiilin takertelua ja jumiutumista ei tarvitse huomioida, jos käytetään palloistukkaventtiileitä, joiden toimintamekanismi on yleensä suunniteltu siten, että takertuminen on epätodennäköistä. Suuntaventtiilissä takerteleminen vältetään mekaanisella pakkotoimisuudella tai erityisentyypisellä patruunamallisella istukkaventtiilillä, joka ei avaudu, jos sitä käytetään yhdessä jonkin muun venttiilin kanssa päävirtausta ohjaamaan. Proportionaalisessa venttiilissä ei voida sulkea pois asetusarvon tahattomasta muutoksesta johtuvia toiminnan muutoksia. Virtaventtiileissä tilavuusvirran muutosta ei huomioida, jos venttiilissä ei ole liikkuvia osia tai jos kyseessä on ei-säädettävät pyöreät aukot, joiden halkaisija on riittävän suuri. Suuntaventtiileissä servo- ja proportionaalisissa venttiileissä hydraulisia vikoja ja niiden aiheuttamia hallitsemattomia toimintoja ei oteta huomioon, jos niitä voidaan arvioida teknisiltä ominaisuuksiltaan samoin kuin perinteisiä suuntaventtiileitä. [30.]

4.3.2 Ohjelmistot

Ohjelmistojen todentaminen ja kelpuutus on myös turvallisuusvaatimusten toteutuksen varmistamista. Standardissa SFS-EN 61508-3 esitellään ohjelmistojen testaustekniikoita. Ohjelmistot testataan useammalla eri tavalla. Yksikkötestauksella tarkastetaan toimiiko yksittäinen ohjelmistomoduuli oikein. Integrintitestaus yhdistää eri moduulit kokonaisuuksiksi ja testaa niiden välisen toiminnan, ja toiminnan kokonaisuutena järjestelmänä. Kun nämä testausvaiheet on käyty läpi, tehdään kelpuutus- ja järjestelmätestaus, joka vastaa vaatimusten toteuttamisen oikeellisuutta. Ohjelmiston kelpuutusta ei voida tehdä irrallisena sen alustana olevasta laitteistosta ja järjestelmän käyttöympäristöstä, joten pelkkä tietokonepohjainen testaus ei riitä. Ohjelmistotestauksen pohjana on usein ohjelmiston systemaattisen kyvykkyuden ja kehittämisenmalli, niin sanottu V-malli (kuva 20.).



Kuva 23 Ohjelmiston V-malli [27]

Todentamisen vaiheesta tehdään suunnitelma, jossa määritellään kriteerit, tekniikat ja työkalut, joilla todentaminen tehdään. Tässä vaiheessa arvioidaan myös turvallisuuden eheyden tasot. Todentaminen pitää sisällään

- ohjelmistojen turvallisuusvaatimusten todentaminen
- arkkitehtuurin todentaminen
- järjestelmäsuunnitelman todentaminen
- moduulisuunnittelun todentaminen
- koodin ja datan todentaminen
- suorituskyvyn todentaminen
- yksikkötestaus
- integraatiotestaus
- hardware-software integraatio
- järjestelmän turvallisuuden kelpuutus ohjelmiston osalta [35].

Testauksen vaiheet ja tulokset on dokumentoitava, myös niissä tapauksissa kun ohjelmisto ei vastaa vaatimuksia.

Kelpuutukseen käytettäviä taulukoita on niin sähköisille, kuin mekaanisille järjestelmille. Näiden avulla voidaan valita hyvin koetellut komponentit ja toimintatavat, joiden avulla järjestelmää voidaan pitää turvallisena.

5 CASE: TURVATOIMINNON SUUNNITTELU PUOMIN VIKAANTUMISEEN

Turvatoiminto suunnitellaan Tampereen teknillisellä yliopistolla, Hydrauliiikan ja automatiikan laitoksella olevaan GIM-koneeseen. Koneen alustana on Avant 365 -pienkuormaaja. Koska Avant 365 -pienkuormaaja on kaupallinen pienkuormaaja, on sen turvallisuus nykyiselläänkin korkealla tasolla. Vastaavanlaisten liikkuvien työkoneiden tapaturmatilastot osoittavat, että pienkuormaajien puomin liike aiheuttaa suurimman osan tapaturmista. Vakavimmat tapaturmat sattuvat liikkuvan puomin ja koneen rungon väliin puristuksiin jäämisestä tai koneen kaatumisesta, mikä voi olla seuraus puomin hallitsemattomasta liikkeestä. Pienkuormaajien vakaus häiriintyy eniten taakkaa siirrettäessä ja puomin ollessa irti koneen kyljestä.

Suomessa pienkuormaajilla sattuneita kuolemaan johtaneita tapaturmia on raportoitu kaksi kappaletta. Työtehoseuralle tehdyssä kyselytutkimuksessa pienkuormainten käytön toiminnallisuudesta ja työturvallisuudesta käy selville, että tapaturmia ja ”läheltä piti” -tilanteita on sattunut noin parisataa vuodessa. Eniten on tapahtunut vaarallisia perännousuja, pienkuormaajan kaatumisia tai melkein kaatumisia. Merkittävä osuus vaaratilanteista kohdistuu myös sivullisiin henkilöihin. [36.] Yhdysvalloissa National Institute for Occupational Safety and Health (NIOSH) on kerännyt tilastoa liukuohjattujen pienkuormainten kuolemaan johtaneista tapaturmista vuosien 1980 – 1997 aikana. Kuolemantapauksia on raportoitu yhteensä 91 kappaletta. 54 tapauksessa ihminen on jäänyt puristuksiin koneen rungon ja puomin tai kauhan väliin. 15 tapauksessa kuolema on johtunut puristuksiin jäämisestä, mutta tilanne on ollut epäselvä. Pienkuormaajan ympäripyörähtäminen on ollut syynä 17 tapauksessa. [37.] Pienkuormaajan etu- tai takaosan nousu on hyvin todennäköistä. Tapahtumista ei ole kuitenkaan rekisteröityjä merkittäviä tapaturmia. Tapahtumamekanismit ovat samat kuin kaatumisessa, mutta jokin muuttuja on pitänyt koneen pystyssä. Toisinpäin ajatellen koneen etu- tai takaosan nousu voi olla riittävä riskitason alentaminen kaatumiselle.

Liikkuvien työkoneiden älykkyyden ja toimintojen lisääntyessä ohjelmistosta tulee yhä kompleksisempi. Älyn lisääntyessä toimintoja on mahdollista valvoa ja analysoida enemmän. Ohjelmistotestaus tulee sitä haasteellisemmaksi mitä laajempi ohjelma on. Reaaliaikainen ja HIL (Hardware-In-the-Loop) -simuloinnissa malli reagoi ulkoa tuleviin käskyihin ja siihen on liitetty osa koneen ohjausjärjestelmää. HIL -simulointia on käytetty apuna erittäin turvallisuuskriittisten järjestelmien testaamiseen, kuten ydinvoimalat, lentokoneet ja satelliitit. Tietokoneiden tehon lisääntyessä simulointia on pystytty

käyttämään hyväksi pienemmissäkin koneissa ja järjestelmissä. Reaaliaikaista mallinusta on ryhdytty käyttämään kuljettajien koulutuksessa ja suunnittelun tukena. HIL-simulointia liikkuvien työkoneiden ohjausjärjestelmien testauksessa ja riskien pienentämisen todentamisessa ja kelpuutuksessa kannattaisi hyödyntää enenevässä määrin.

5.1 Turvatoiminnon määritteleminen

Pienkuormaajien aiheuttamat yleisimmät tapaturmat ovat koneen kaatuminen, käyttäjän puristuksiin jääminen sekä sivullisten henkilöiden alle jääminen. Kaupallisille pienkuormaajille on tehty riskianalyysit, ja todettu jäännösriskit siedettäviksi. Koneen raja-arvot on määritelty ja koneen toiminnot on jaettu osatoiminnoiksi. Tapaturmatilastoista voidaan yhä todeta pienkuormaajan yhdeksi suurimmaksi riskiksi koneen kaatumisen. [35; 36]

VAARALLINEN TAPAHTUMA = Koneen kaatuminen

Tiedetään, että pienkuormaajan vakaus on heikoin silloin, kun puomi kannattelee kuormaa ja puomi on ajettu ääriasentoon rungosta poispäin. Pienkuormaajan kaatumisen todennäköisin syy on puomin asento. Kun käyttäjä nostaa taakkaa ja tuntee koneen käyvän epävakaaksi, liike voidaan pysäyttää ja kaatuminen typistyy peräosan nousuun. Jos vakauden häiriintymistä ei havaita, tai puomin liikettä ei saada pysäytettyä voi tapahtuma johtaa koneen kaatumiseen.

VAARAN ALKUPERÄ = Puomin hallitsematon liike

Vaaran alkuperä ja vaarallinen tapahtuma on käsitelty riskianalyysissa. Riskin pienentämiseksi käytetään ensisijaisesti luontaisesti turvallisia suunnittelutoimenpiteitä. Pienkuormaajassa on ylikuormahälytin, jolloin kuljettaja ei voi huomaamattaan ottaa kyytiin liian isoa taakkaa. Vakaajan avulla kuorma pidetään vaakatasossa koko puomin liikerradan ajan. Hydraulikkakomponentit ovat standardien mukaan valmistettuja ja määräysten mukaan asennettuja, jolloin niitä voidaan pitää hyvin koeteltuina komponentteina. Kuormanlaskuventtiili takaa kuorman pysymisen ylhäällä. Jäykkä keskinivel vähentää kaatumisvaaraa. Ohjaamossa olevaa kuljettajaa on suojaamassa turvakaari, joka on testattu kestämaan ympäripyörähtämistilannetta. Pienkuormaajassa on hätäpysäytyspainike, joka pysäyttää myös teleskooppipuomin liikkeen. Pienkuormaajan puomin tapauksessa luontaisesti turvallisia suunnittelutoimenpiteitä ovat oikea painetaso, kuormanlaskuventtiilin sijoittaminen järjestelmään, hyvin koeteltujen komponenttien käyttäminen sekä letkujen ja muiden hydraulikkomponenttien oikea mitoitus. Hyvin suunniteltu ja testattu ohjausjärjestelmä on myös osa luontaisesti turvallista suunnittelua. Luontaisesti turvallisilla suunnittelutoimenpiteillä ei riskiä saada pienennettyä riittävästi. Pienkuormaajissa onkin turvatoimenpiteenä esimerkiksi hälytys ylikuormasta. Käyt-

täjä ei voi nostaa huomaamattaan liian suurta kuormaa, mikä häiritsee vakautta. Jäänösriski on huomioitu käyttäjien koulutuksessa ja varoituksina käyttöohjeissa.

Tilastot kuitenkin osoittavat, että tapaturmia sattuu turvatoiminnoista huolimatta. Näiden tilastojen valossa tehdään uudelleen riskianalyysi puomin hallitsemattomasta liikkeestä. Luvussa 4.1. esitetään tapaturman riskitason määrittäminen. Käyttäjäkokenuksista päätellen puomin hallitsematon liike voidaan jakaa kahteen tilanteeseen:

- Puomin hallitsematon liike on hyvin mahdollinen mutta seuraukset eivät ole vakavia, tai
- puomin hallitsematon liike, jos sitä ei saada pysähtymään, voi johtaa kuolemaan, mikä tosin on epätavallista.

Kuvissa 16 ja 17 on asteikot vaarallisen tapahtuman todennäköisyydestä ja seurausten vakavuudesta. Näiden kuvien mukaan lasketaan tilanteiden a) ja b) riskitasot. Todennäköisyysarvio tilanteessa a) perustuu tapaturmatilastoihin. Puomin hallitsemattomia liikkeitä sattuu mahdollisesti vielä enemmän, mutta niistä ei ole raportoitu mihinkään. Riskitason määrittely lasketaan $8 \times 20 = 16$. Tilanteen b) todennäköisyysarvio perustuu kuolemaan johtaneiden tapaturmien määrään. Tapahtuma ei ole yleinen, mutta sen satuesssa tapaturmaan johtaneet syyt eivät ole yllättäviä. VTT:n julkaisemassa raportissa käsitellään suuntaventtiilin vikaantumista, ja venttiilin takertuminen auki voi tapahtua työkoneen käyttöön puitteissa [r]. Riskitason määrittely lasketaan $0,4 \times 100 = 40$. Riskitaso on näin ollen joko kohtalainen tai merkittävä. Molemmissa tapauksissa riskin pienentäminen on tavoiteltavaa.

RISKITASO = Merkittävä

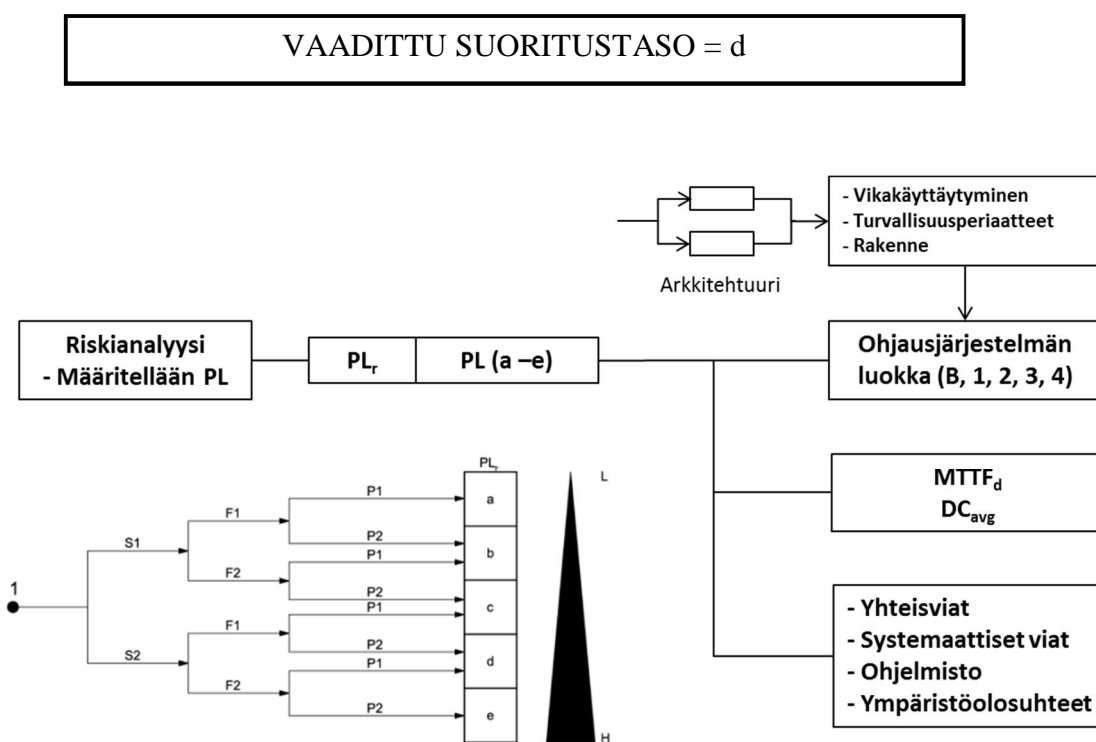
Pienkuormaajan kaatumisen riskiä on pienennetty luontaisesti turvallisilla suunnittelu-toimenpiteillä. Koneeseen on lisätty turvatoimintoja anturien ja ohjelmoitavan elektronikan kautta. Voidaanko ohjausjärjestelmällä toteuttaa lisää turvatoimintoja, jotka vähentävät pienkuormaajan kaatumisen riskiä? Taulukossa 9 on tehty alustava riskin analysointi ja suoritustason määrittäminen luvun 3.3.1 kuvan 10 mukaan.

Alustava riskin analysointi									
Toiminto		Vaaralliset olosuhteet				Riskin suuruuden arviointi			
Nro	Toiminto	Vaara	Vaaratilanne	Vaarallinen tapahtuma	Mahdollinen vahinko	S1/S2	F1/F2	P1/P2	PL
x.xx	Puomin nosto	Liikkuva osa	Koneen käyttäminen kuorman kanssa	Liikkuvien osien pysähtymisen vikaantuminen Hallitsemattomat liikkeet	- Kuorman tippuminen - Vakauden menetys - Puristuminen	S2	F1	P2	d

S = vamman vakavuus, F = vaaralle altistumisen taajuus, P = mahdollisuus välttää vaaraa, PL = suoritustaso

Taulukko 9 Alustava riskin analysointi

Käytettävä suoritustaso tulee määritellä olemassa olevasta järjestelmästä. Suoritustason määrittämiseen vaikuttavat useat muuttujat ja järjestelmän ominaisuudet (kuva 21). Vaaditulle suoritustasolle PL_r päästään kappaleessa 3.3.1 kuvan 12 mukaan luokalla 2, jos diagnostiikan kattavuus on 90 - 98 % tai vaihtoehtoisesti luokalla 3. Luokassa 2 ohjausjärjestelmän on testattava automaattisesti turvallisuuteen liittyvän ohjausjärjestelmän osan virheetön toiminta.



Kuva 24 Suoritustason määrittäminen [29]

Luokka 2 on yksikanavainen rakenne, mutta siinä tulee tehdä testaus komponentin/logiikan toiminnalle. Luokan 3 yleisenä vaatimuksena on, että mikään yksittäinen vika ei saa aiheuttaa turvatoiminnon menettämistä.

Standardin SFS-EN ISO 13849-1 liitteen C mukaan yksittäiselle hydraulikomponentille $MTTF_d$ arvona voidaan käyttää arvoa 150 vuotta jos

- komponentit on valmistettu noudattamalla turvallisuusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita standardin SFS-EN ISO 13849-2 mukaisesti
- komponentin valmistaja erittelee hyödyntäjälle soveltuvat käyttötarkoitukset.

Pienkuormaajan kaatumiseen johtavan puomin hallitsemattoman liikkeen syiksi katsottiin joko väärän liikkeen havaitsemisen puute tai liikkeen pysäyttämisen estyminen. Havaitsemiseen voidaan vaikuttaa diagnostiikkaa lisäämällä. Puomin liikkeeseen ja sen pysäyttämiseen vaikuttaa kaksi komponenttia: hallintalaite ja suuntaventtiili. Hallinta-

laitteelta täytyy tulla pysäytyskäsky ja suuntaventtiilin täytyy toteuttaa se. Kuvassa 22 on ohjaus- ja pysäytyskäskyn reitti.



Kuva 25 Puomin liikkeeseen vaikuttavat tekijät

Hallintalaitteelta suuntaventtiilille ohjauskäsky menee sähköisenä, suuntaventtiililtä sylinterille hydraulisena. Kun liikettä ei saada pysäytetyksi, hallintalaite ei joko lähetä pysäytyskäskyä tai suuntaventtiili ei toteuta käskyä. Taulukossa 10 on eritelty syyt miksi puomia ohjaavan sylinterin liike ei pysähdy ja voidaanko syy havaita

Nro	Vika	Tapahtuma	Voidaanko havaita
1	Hallintalaite rikki	Hallintalaite ei lähetä pysähtymiskäskyä	K
2	Hallintalaitteen kontakti huono	Hallintalaite ei lähetä pysähtymiskäskyä	K
3	Sähköjohto hallintalaitteen ja suuntaventtiilin välillä	Suuntaventtiili ei saa pysäytyskäskyä	K
4	Suuntaventtiilin kela rikki	Suuntaventtiili ei toteuta pysähtymiskäskyä	K
5	Suuntaventtiilin jousi rikki	Jousi ei palauta suuntaventtiiliä keskiasentoon	E
6	Suuntaventtiilin karan jumittuminen	Suuntaventtiilin kara ei liiku pysähtymiskäskyn mukaisesti	E

Taulukko 10 Puomin sylinterin pysähtymiseen vaikuttavat tekijät

aistihavainnoin tai komponenttien sekä ohjelmoitavan elektroniikan sisäänrakennettujen diagnostiikkamenetelmien avulla.

Diagnostiikan kattavuus on riippuvainen pienkuormajasta ja sen ohjausjärjestelmästä. Taulukosta 10 katsottuna vikaantumistilanteista neljä voidaan havaita, ja kahta ei voida havaita. Diagnostiikan kattavuus on näin ollen 67 %. Jotta päästään vaaditulle suoritus- tasolle, on parannettava diagnostiikan kattavuutta tai toteutettava puomin pysäyttäminen ohjausjärjestelmässä luokan 3 vaatimusten mukaisesti.

Puomin pysäyttämisen ja diagnostiikan heikkouden pääkomponentti on suuntaventtiili. Venttiilin toimintaa ei ole mahdollista tarkistaa siinä merkityksessä, kuin luokka 2 vaatii. Turvallisuuden parantaminen ja riskin pienentäminen vaatii luokan 3 vaatimusten

täyttämistä ja jos samalla voidaan parantaa diagnostiikan kattavuutta, toteutettava suoritustaso voi olla jopa e.

RISKIN PIENENTÄMINEN

- Ohjausjärjestelmän luokka 3
- Diagnostiikan kattavuus > 90 %

Näitä parannuskeinoja ei voida toteuttaa mekaanisesti, sähköisesti tai hydraulisesti. Riskin pienentäminen on mahdollista toiminnallisen turvallisuuden keinoin.

5.2 Turvatoiminnon suunnittelu ja toteuttaminen

Riskin pienentämisprosessin tuloksena saadaan ohjausjärjestelmälle seuraavat turvallisuusvaatimukset:

- puomin liike voidaan pysäyttää kaikissa tilanteissa
- pysäyttämisen estävät viat on havaittava niin, että niihin voi reagoida.

Tämä tarkoittaa sitä, että suuntaventtiilin viat tulisi havaita ennen kuin ne ehtivät aiheuttaa vahinkoa. Tutkitaan tilannetta, jossa venttiili on jäänyt auki asentoon. Tämä on mahdollista silloin, kun venttiilin kela vaurioituu tai ohjauskaran ja kotelon väliin pääsee epäpuhtauksia. Kelan vaurioituminen on mahdollista huomata sähköisesti, mutta karan jumittumisen huomioiminen ennen vikatoimintoa on vaikeampaa. Ilman simulointimallia turvatoiminnon todentaminen olisi lähes mahdotonta. Täytyy tuntea järjestelmän käyttäytyminen vikatilanteessa, jotta ohjelman logiikka saadaan toimimaan oikein ja se on testattava.

Pienkuormaajan riskianalyysin mukaan vakavimmissa riskeissä yhteisenä tekijänä on hydraulisen suuntaventtiilin väärä toiminto. Suuntaventtiilin vika on harvinainen, mutta odotettavissa oleva. Hydrauliikan suurin yksittäinen vioittumisen syy ovat epäpuhtaudet, jotka aiheuttavat esimerkiksi venttiilien takertelua. Tällaisen vian saaminen oikeaan järjestelmään ei ole toivottavaa, eikä sitä voida varmuudella ja haluttaessa aiheuttaa.

Ilman simulointimallia tehtävä turvatoiminto jää hydrauliikkajärjestelmien tuntemuksen ja olettamuksien varaan. Simulointimallilla suuntaventtiilin vikamuodot saadaan aiheutettua todenmukaisesti, ja aina silloin kuin halutaan. Simulointimallista antaa viitteitä vian vaikutuksesta koko järjestelmään.

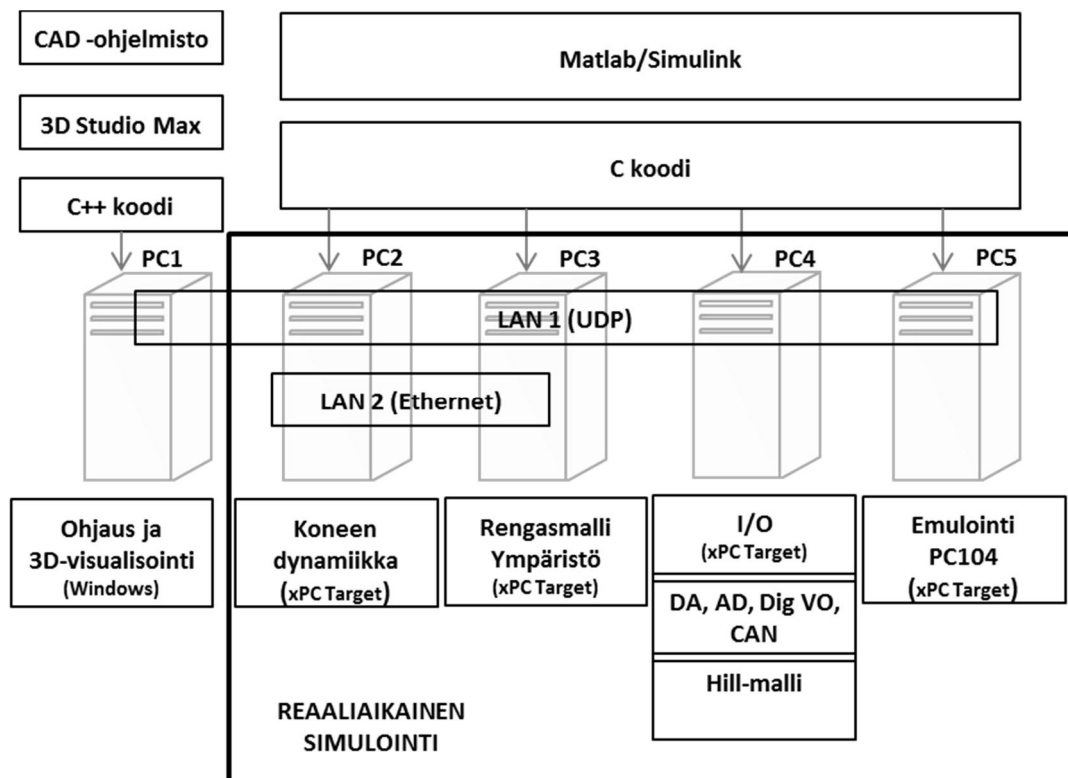
Ennen kaikkea simulointimallilla testaaminen on turvallista. Jos kara jää epäpuhtauden takia auki, ohjauskäsky ei vaikuta venttiiliin. Suuntaventtiili läpäisee tilavuusvirran ja puomin liike jää päälle, tai jos puomi on ajettu päätyasentoon, niin paineet sylinterin kammiossa nousevat ja lopulta tilavuusvirta ohjautuu paineenalennusventtiilin läpi. Vaikka puomi ei tässä tilanteessa enää liiku, varaa se järjestelmästä painetta ja tilavuus-

virtaa, eikä muut työliikkeet, mukaan luettuna ohjaus, saa enää täyttää kapasiteettia. Taulukossa 11 on esitettyä käyttötapauskaavio suuntaventtiilin jumiutumisen ja tapahtuman suoritustason määrittymisestä ja riskiin liittyvät muuttujat.

Nro	Tapaturmaskenaario	Tiedossa olevat suojaustoimenpiteet	Se	Fr	Pr	Av	PL	Ehdotetut uudet suojaustoimenpiteet
Käyttötapaus: Puomin liikkeellä nostetaan taakka ylös								
	Suuntaventtiili jumittuu auki asentoon, eikä puomin liike pysähdy pysäytymiskäskystä	Puomin liikkeen saa pysähtymään joko hallintalaitteesta tai moottorin sammuttamalla.	4	2	2	3	d	Kuljettajalle tieto miksi puomin liike ei pysähdy. Lisätään diagnostiikkaa, jolloin tieto vikatilanteesta tulee niin nopeaan, että kuljettaja ehtii reagoida ennen vahinkoa.

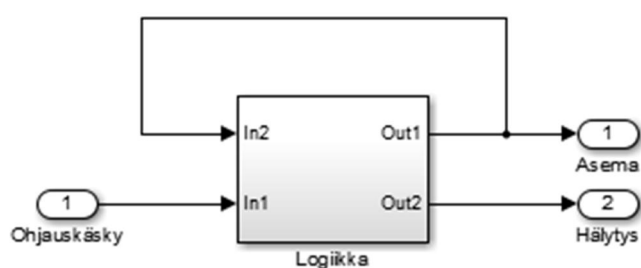
Taulukko 11 Käyttötapauskaavio

Turvatoiminto suunniteltiin GIMsim -simulointimallilla, mikä koostuu viidestä lähiverkkoon kytketystä tietokoneesta. Neljä tietokonetta pyörittää reaaliaikaista simulointimallia ja yksi hoitaa ohjauksen ja visualisoinnin (kuva 26). Simulointimallit ovat rakennettu Matlab ja Simulink ohjelmien päälle. GIMsim -järjestelmä on rakennettu käyttämällä tavallisia kaupallisia ohjelmistoja ja tietotekniikkakomponentteja. Järjestelmällä halutaan osoittaa, että reaaliaikainen simulointi ja sen tuomat hyödyt voidaan tuoda koneenvalmistajien käyttöön.



Kuva 26 Periaatteellinen malli GIMsim -simulointijärjestelmästä [38]

Simulointimalli on rakennettu vastaamaan tutkimuskäytössä olevaa GIM-konetta. GIM-kone perustuu Avant 635 -pienkuormaajaan. Se on runko-ohjattu suljetun piirin työko-
ne, jossa työlaitteina ovat puomi, teleskooppi ja kauha tai trukkipiikit. Kuvassa 28 on
esitetty GIM-koneen työhydrauliikkapiiri puomille. Simulointimalliin suunnitellaan
lisäys pienkuormaajan ohjelmistoon. Turvatoiminto tarkkailee hallintalaitteelta tulevaa
ohjauskäskyä ja puomin kulma-anturia. Jos ohjauskäskyä ei tule, ja puomin kulma-
anturi lähettää muuttuvaa signaalia, liikkuu puomi virheellisesti. Kulma-anturin signaa-
lista tulee suodattaa pois hydrauliikan aiheuttama jousto, niin kuorman kuin maaston
vaikutuksestaakin. Puomin ohjauksesta saadaan näin takaisinkytketty malli (kuva 27).

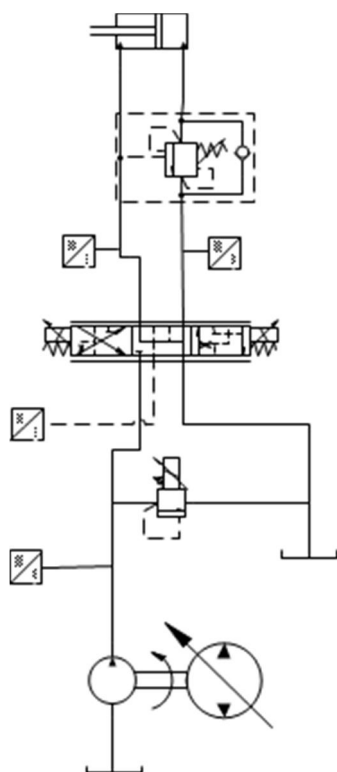


Kuva 27 Puomin liikkeen tarkkailun malli

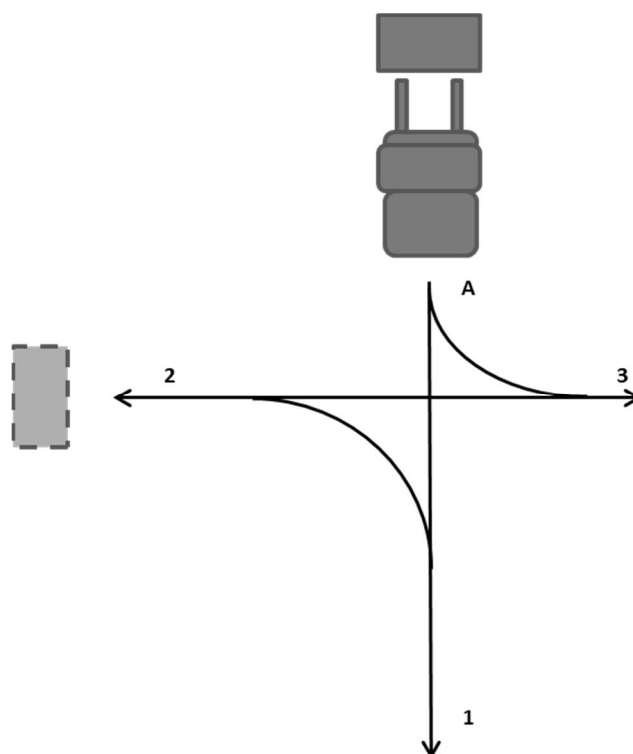
Simulointimalliin nauhoitettiin pienkuormaajalle tyypillinen työkierto (kuva 29), jota
voitiin toistaa samanlaisena koko tutkimuksen ajan. Työkierto voi kuvata joko taakan
nostoa maasta ja jättöä korkealle hyllylle (trukkitoiminto), tai taakan nostoa maasta ja
kippausta korkean laidan yli (maatalouskoneet).

Työkierron vaiheet ovat:

- A Taakka nostetaan maasta.
- 1 Peruutetaan suoraan.
- 2 Vaihdetään suunta, ajetaan eteenpäin ja käännetään oikealle, pysähdytään.
Ajetaan puomi ja teleskooppi päätyasentoon ja jätetään taakka ylhäällä.
- 3 Lasketaan puomi, teleskooppi ajetaan sisään ja peruutetaan suoraan.
- A Vaihdetään suunta, ajetaan eteenpäin oikealle kääntyen takaisin lähtöpaik-
kaan.



Kuva 28 Puomin
hydraulijärjestelmä



Kuva 29 Pienkuormaajan työkierto

Testaus aloitettiin suunnittelemalla työkierto ja ajamalla tätä simulointimallilla. Työkierto nauhoitettiin simulointimalliin ja vikojen testaus toteutettiin työkierrolla, joka oli samanlainen kaikissa tapauksissa. Ohjausventtiilin karan jumiutuminen auki asentoon saadaan aikaiseksi muuttamalla yhtä simulointimallin parametria. Suuntaventtiilin todennäköisin hetki jäädä auki epäpuhtauden takia on siinä tilanteessa, kun venttiili avataan työkierron mukaan. Tässä tapauksessa suuntaventtiili voi jäädä auki työkierron alussa, kun taakka nostetaan, tai puolivälissä, kun puomi ja teleskooppi ajetaan pääty-asentoon ja taakka jätetään pois tässä asennossa.

Testaus osoitti, että taakkaa jättäessä vika ei aiheuta suurta vaaraa. Puomi ajautuu pääty-asentoon täydellä teholla ja se aiheuttaa pientä epävakautta pienkuormaajassa. Vika myös huomataan nopeasti, kun puomia ei saada liikkumaan päätyasennosta alaspäin, vaikka vian alkuperää ei tunnistettaisikaan. Koska taakka on jätetty tässä kohtaa pois, ei tilanne aiheuta häiriötä koneen vakauteen. Kun vika on havaittu, koneen ajonopeutta voi pienentää. Suurin vaaratilanne aiheutuu, jos puomi törmää korkealla olevaan esteeseen.

Vian vakavuus käy ilmi, kun taakka nostetaan maasta ajokorkeuteen ja pienkuormaajalla lähdetään peruuttamaan. Peruuttaminen tapahtuu normaalisti kiihdyttäen, kun oletetaan että puomia on ajettu vain vähän ylöspäin ja taakka pysyy hieman irti maasta. Täl-

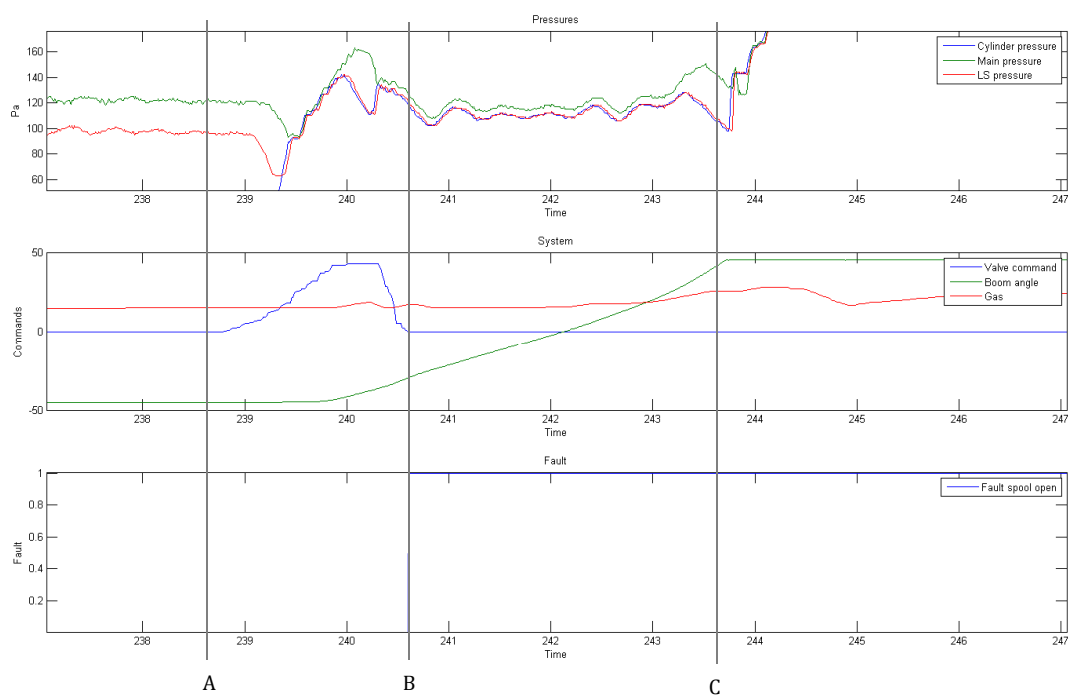
löin työkonteen vakaus on hyvä ja normaalille ajolle ei ole estettä. Simulointimallissa tehty testaus osoittaa, että kun puomin liike ei pysähdy normaalisti peruutettaessa, pienkuormaajaan vakaus menetetään. Simulointimallilla tehdyissä testeissä pienkuormaaja kaatui jokaisella simulointikerralla. Kaatumiseen johtaneet syyt ovat:

- liian suuri nopeus
- kuljettajan huomio on peruutussuunnassa
- kuljettajalla ei ole aikaa reagoida tapahtuneeseen.

Todellista työkiertoa ajatellen taakkaa maasta nostettaessa kuljettajan katse ja huomio ovat kiinnittyneet peruutettavaan suuntaan. Kiihdytysvoimat ja taakan nouseminen ääriasentoon muuttavat pienkuormaajan tasapainoa niin että kuormaaja kaatuu. Kuljettajan havaitessa pienkuormaajan epävakauden hänen reaktionsa todennäköisesti ovat kuormaajan ajon pysäyttäminen ja puomin hallintalaitteeseen vaikuttaminen. Epäpuhtaus karan välissä estää suuntaventtiilin toiminnan ohjauskäskyn mukaisesti, eikä puomin liike pysähdy. Hallintalaitteen lisäksi kuljettajan vaihtoehtoiset mahdollisuudet puomin liikkeen pysäyttämiseksi ovat:

- a) dieselmoottorin sammuttaminen
- b) hätäpysäytyksen käyttäminen.

Molemmilla toiminnoilla puomin liike saadaan pysäytetyksi. Tarkasteltavan tilanteen ongelmana on ajan puute. Kuljettajalla ei ole aikaa tehdä näitä vaihtoehtoisia pysäytys-toimintoja jos hän on ensin yrittänyt pysäyttää liikettä hallintalaitteella.

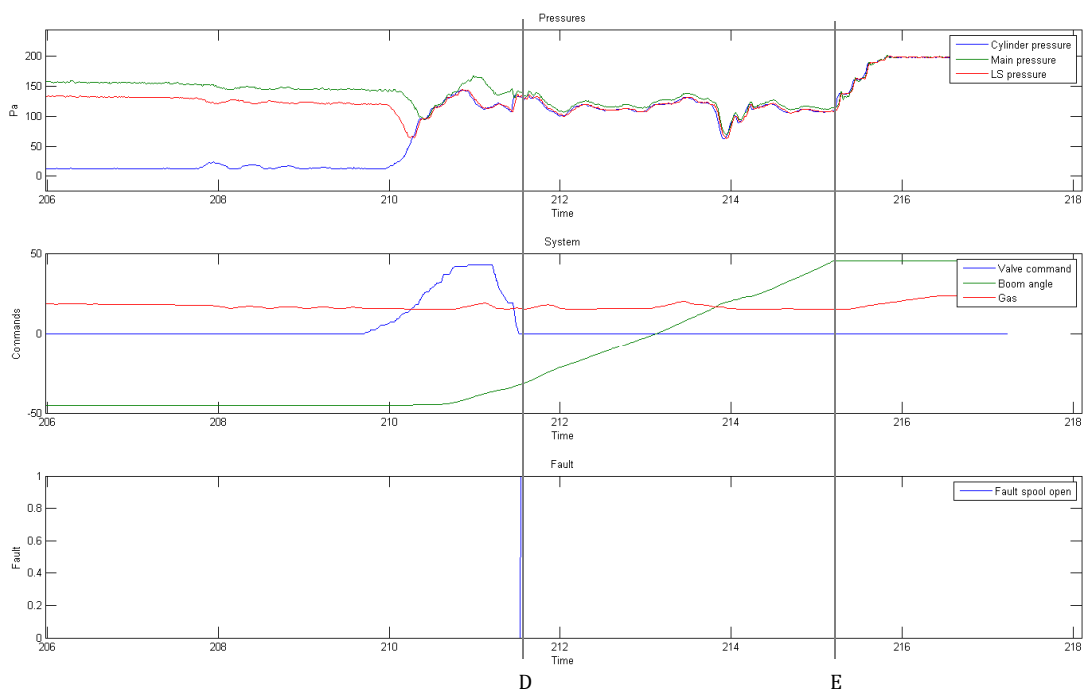


Kuva 30 Kuvaajat pienkuormaajan käyttäytymisestä vikatilanteessa

Kuvasta 30 nähdään, kuinka kohdassa A annetaan ohjauskäsky taakan nostamiseksi, ja paineet nousevat. Kun ohjauskäsky loppuu, mutta puomin kulma jatkaa kasvamistaan, tunnistetaan vika. Järjestelmä tunnistaa vian kohdassa B, ja kun konetta aletaan peruuttaa ja puomin kulma jatkaa kasvuaan saavuttaen päätyasennon kone muuttuu epävakaksi ja kaatuu kohdassa C. Virheellisen toiminnon ja kuormaimen kaatumiseen välissä on kolme sekuntia aikaa.

Simuloinnin avulla voidaan todeta, että ohjauskaran jumiutuminen auki asentoon, ja puomin liikkeen jatkuminen, yhdistettynä normaaliin työkierron vaiheeseen saa pienkuormaajan kaatumaan lähes varmasti. Voidaanko vian tunnistamisen avulla käyttää nuo kolme sekuntia niin, että kuormaajan kaatuminen saadaan estettyä?

Simulointimallia muutettiin vielä niin, että karan auki jumiutumisesta aiheutuu hälytys, ja vian ilmaantuessa kuormaajalle annetaan pysähtymiskäsky. Tätä lisätoimintoa tutkittiin saman, simuloinnin alussa nauhoitetun työkierron avulla. Kuvassa 31 on kuvaajat tilanteesta, jossa vian ilmaantuminen pysäyttää kuormaajan. Kuvaajien kohdassa D karan jumiutuminen huomataan ja kohdassa E puomi on liikkunut yläasentoon. Ylimmän kuvaajan paineista voidaan huomioda paljon stabiilimpi käyttäytyminen kuin kuvan 30 tapauksessa. Puomin liikkeen jatkuminen ja kuormaajan pysäyttäminen häiritsevät jonkin verran koneen vakautta, mutta vian tunnistaminen ja siitä seuraava pysäytyskäsky pystyvät estämään kuormaajan kaatumisen.



Kuva 31 Kuvaajat pienkuormaajan käyttäytymisestä kun viasta saadaan ilmoitus

Vian havaitseminen antaa kuljettajalle aikaa reagoida tapahtuneeseen, tai oikeellisen vian tunnistamisen kautta ohjausjärjestelmällä voi toteuttaa suojaustoimenpiteen automaattisesti.

5.3 Turvatoiminnon arviointi

Todentaminen tarkoittaa todistettavasti oikeaa, tehokasta menetelmää tai perusteellista simulointia ja testauksen havainnollistamista. Turvatoiminnon toteutuksen arviointi alkaa vaatimusten määrittelystä. Luvussa 5.2. määriteltiin, että

- puomin liike tulee pystyä pysäyttämään kaikissa tilanteissa
- pysäyttämisen estävät viat on havaittava niin että niihin voi reagoida.

Puomin liike on pysäytettävissä hallintalaitteella, sammuttamalla dieselmoottori ja tekemällä hätäpysäytys. Normaalissa käyttöolosuhteessa ensisijainen pysäyttämistapa on hallintalaitteeseen vaikuttaminen. Pysäyttämistä estävät viat ovat sähköisiä, hydraulisia tai ohjelmallisia.

Sähköiset viat ovat hallintalaitteen tai suuntaventtiilin vikoja. Komponenttien oman diagnostiikan, tai ohjelmoitavan elektroniikan diagnostiikan, kautta nämä viat ovat havaittavissa, ja niihin voidaan reagoida ennen, kuin vakavaa vaaratilannetta syntyy. Ohjelmalliset viat ovat ohjausjärjestelmän systemaattisia vikoja, jotka on löydettävä ja korjattava ohjelmistotestauksen varhaisessa vaiheessa.

Hydrauliset viat voivat olla letkun irtoaminen tai puhkeaminen. Letkurikko on helppo havaita ja puomin hallitsematon liike on estettävissä letkurikkoventtiilillä. Ohjausventtiilin hydraulisia vikoja on vaikeampi havaita siinä ajassa, että reagointi on mahdollista. Ohjausventtiilin karan takertelut tai jumiutuminen ovat havaittavissa siinä vaiheessa, kun yritetään muuttaa karan tilaa.

Reaaliaikaisen simuloinnin avulla huomattiin, että tapaturmien ehkäisyssä tämä on liian myöhäinen vian havaitsemisaika. Tarkkailemalla ohjauskäskyjä ja toimilaitteiden tiloja, voidaan väärä toiminta havaita aiemmin kuin käyttäjän havaintoihin perustuen. Simuloinnin avulla voidaan todeta, että puomin liikettä ja ohjauskäskyä tarkkailemalla ohjausventtiilin vika voidaan havaita niin, että siihen voi reagoida tapaturman välttämiseksi. Reaaliaikaisen HIL -simulointijärjestelmän avulla voidaan tehdä kelpuutustestaukset, ja saada riittävä arvio siihen, toteuttaako turvatoiminto turvallisuusvaatimukset.

Vaaditulle suoritustasolle pääsemiseksi tarvittiin diagnostiikan kattavuuden parantamista, tai luokan 3 ominaisuuksien saavuttamista. Ohjausventtiilin jumiutumisen tunnistaminen nostaa diagnostiikan kattavuutta. Taulukon 10 mukaisesti tämän muutoksen jälkeen kaikki viat ovat tunnistettavissa. Diagnostiikan kattavuudessa päästään seuraavalle tasolle, joka on 90 – 99 %. Luokan 3 arkkitehtuuri vaatii ohjausyksikön valvontaa logiikalla. Tämä toteutuu kun tarkkaillaan puomin aseman muutosta ja ohjausyksiköltä tulevaa ohjauskäskyä. Olemassa oleva suoritustaso on vaadittavan suoritustason mukai-

nen. Merkittävä riski koneen kaatumiselle on pienentynyt. Riski on yhä olemassa, mutta esiintymistodennäköisyys on pienentynyt diagnostiikan kattavuuden myötä. Taulukossa 12 on esitetty havaitut riskit ja tehdyt toimenpiteet.

Riskin analysointi riskin pienentämisen jälkeen								
Toiminto		Riski	Riskin pienentäminen	Toimenpiteen jälkeisen riskin suuruuden arviointi				
Nro	Toiminto	Vaarallinen tilanne	Tehty toimenpide	S1/S2	F1/F2	P1/P2	PL	Riski-luokka
x.xx	Puomin nosto	Puomin liikettä ei saada pysäytetyksi ohjausventtiilin jumiutumisen takia	Vertaillaan puomin aseman muuttumista ja ohjauskäskyä. Jos asema muuttuu ilman ohjauskäskyä annetaan järjestelmälle tieto vikatilanteesta	S2	F1	P1	c	3

S = vamman vakavuus, F = vaaralle altistumisen taajuus, P = mahdollisuus välttää vaaraa, PL = suoritustaso

Taulukko 12 Riskin analysointi pienentämisen jälkeen

Voidaan todeta, että turvatoiminnon jälkeen vaadittava suoritustaso on alhaisempi kuin saavutettu suoritustaso. Riskiluokka on alentunut merkittävästä riskistä kohtalaiseen riskiin. Tehtyjen toimenpiteiden jälkeen voidaan riskin olemassaolo hyväksyä.

6 TULOKSET

Luvussa 5 esitellyn turvatoiminnon suunnittelun lähtökohta oli simulointimallin käyttäminen turvatoiminnon arvioinnissa. Turvatoiminto suunniteltiin ja toteutettiin pienkuormaajan puomin hallitsemattoman liikkeen riskin merkityksen pienentämiseksi. Simuloinnin avulla voitiin havaita ne tilanteet, joissa puomin hallitsemattomasta liikkeestä aiheutui vaaraa. Turvatoiminnon tarpeellisuus ei tullut esille pelkällä analysoinnilla. Simuloinnin tarkoitus on löytää ja tarkastella niitä tilanteita, jotka ovat vaarallisen tapahtuman lähtökohtia.

Puomin hallitsemattoman liikkeen estämiseksi tehdyn turvatoiminnon testaus ei olisi ollut mahdollista todellisella koneella. Vaarallinen vikaantuminen on monien sattumien summa, ja niiden systemaattista esiintymistä koneessa ei ole mahdollista aiheuttaa. Simulointi osoitti myös, että vaarallisen vikaantumisen seuraukset olisivat altistaneet testaajan tapaturmalle. Näennäisesti pienkuormaaja on turvallinen ilman nyt toteutettua turvatoimintoakin, mutta simulointi osoitti, että jos puomin liikettä ei saada pysäytetyksi tietyssä työkierron vaiheessa, riski pienkuormaajan kaatumiseen on erittäin suuri. Vikatilanteen sattuessa reagointiaikaa ei ole riittävästi, jotta vaihtoehtoisia tapoja voitaisiin käyttää puomin liikkeen pysäyttämiseksi.

Työkoneen käyttäjän toiminta vikatilanteessa on tapaturman sattumisen kannalta keskeinen tekijä. Liikkuva työkone voidaan osoittaa turvalliseksi, mutta mitä tarkemmin käyttäjälle voidaan vika ilmoittaa, tai mitä enemmän työkoneen turvalliseksi saattamista on automatisoitu, sitä paremmin tapaturmat voidaan estää. Jos käyttäjän huomio on siirtynyt pois tehtävästä, ilman erillistä hälytystä ei käyttäjä ehdi reagoida ilmenneeseen vikaan ennen kuin vika johtaa vaaralliseen tapahtumaan. Jos reagointiaika on lyhyt, on automatisoidut turvatoiminnot pienentävät riskiä.

Automatisoidut toiminnot ja riskin pienentäminen toiminnallisen turvallisuuden keinoin vaativat turvatoiminnon todentamista ja kelpuutusta. Kelpuutustestausta ei voida tehdä irrallisena osana liikkuvasta työkoneesta ja sen käyttöympäristöstä. Kun kyse on turvallisuuskriittisestä toiminnasta ja testaus oikealla koneella aiheuttaa vaarallisia tilanteita testaajille on reaaliaikainen simulointi paras tapa tehdä kelpuutustestaus. HIL -simuloinnilla voidaan olla varmoja oikeellisesta toiminnasta lähes kaikissa tilanteissa ja simuloinnin kautta voidaan vaarallinen vikaantuminen saada aikaan silloin kuin se on testauksen kannalta oleellista.

Ohjelmistovirheiden vaikutusta koko järjestelmään on vaikea arvioida ennakkoon. Ohjelmisto, joka toimii virheettömästi testausvaiheessa, voi aiheuttaa ongelmia koneessa. Monimutkaisessa järjestelmässä, yhteisvirheiden vaikutuksia kaikissa olosuhteissa, on mahdotonta ennakoida ja hallinnoida. Liikkuvien työkoneiden suunnittelussa, toteutuksessa ja käyttöönotossa on yhdistettävä mekaaniset, hydrauliset, sähköiset ja ohjelmalliset toiminnot. Toimintojen yhdistäminen, kokonaisuuden hallinnoiminen, riskienhallinta ja testaus vaativat ammattitaitoa ja hyvin johdettua ja tehtyä työtä. Liikkuvien työkoneiden turvallisuus koko elinkaaren aikana on haasteellinen prosessi.

Tapaturmatilastot osoittavat, että liikkuvien työkoneiden turvallisuudessa on aukkoja. Simulointi on lisääntynyt koneensuunnittelussa kehittyneen tietotekniikan kautta. Enää mallien pyörittämiseen ei tarvita supertietokoneita. Turvallisuusnäkökulmasta tehty simulointi ei ole enää vain ydinvoimaloiden tai avaruustekniikan käytössä. HIL -simuloinnilla on mahdollista nostaa liikkuvien työkoneiden turvallisuustasoa ja vähentää jäännösriskien vaikutusta työkoneeseen. HIL -simuloinnin hyödyt turvallisuussuunnittelulle ovat:

- Virheet on mahdollista löytää aikaisessa suunnittelun vaiheessa, jolloin ne ovat helpommat ja halvemmat korjata.
- Turvallistamistoimenpiteet voidaan kohdentaa oikeille alueille.
- Ohjelmistotestauksen riskit pienenevät.
- Turvallisuuskriittisten komponenttien toiminnan ja soveltuvuuden testaaminen ilman vaaran aiheutumista henkilöille tai työkoneelle.

7 YHTEENVETO

Liikkuvan työkonteen turvallisuus määritellään koneasetuksessa (400/2008). Liikkuvan työkonteen valmistajan tulee pystyä osoittamaan, että kone täyttää asetuksen vaatimukset. Vaatimuksenmukaisuus täyttyy, jos liikkuva työkone on suunniteltu yhdenmukaisesti standardien mukaan. Vaatimustenmukaisuus ja standardien noudattaminen pystytään osoittamaan erilaisin dokumentein, jotka valmistuvat koneensuunnittelun, testauksen ja käyttöönoton aikana.

Turvallisuuden suunnittelu ja määrittely muodostavat kehämäisen prosessin, joka tarkentuu kierros kierrokselta. Prosessia ei käydä läpi vain koneensuunnittelun vaiheessa, vaan sen tulee seurata työkonetta koko sen elinkaaren ajan. Liikkuvan työkonteen hydraulikkajärjestelmästä ja ohjausjärjestelmästä tulee olla määriteltynä ja dokumentoituna seuraavat turvallisuuteen liittyvät osiot.

1) Riskianalyysi

- a) Liikkuvan työkonteen raja-arvot
 - i) Mahdollisimman selkeä kuvaus työkonteen mekaanisista ja fyysisistä ominaisuuksista, suorituskyvystä, tarkoitetusta käytöstä ja ennakoitavissa olevasta väärinkäytöstä sekä toimintaympäristöstä.
 - ii) Dokumentoituna piirustuksia, laskennallisia arvoja ja käyttötapauksia.
- b) Vaarojen tunnistaminen
 - i) Kaikki mahdolliset vaaratilanteet mekaanisista, hydraulisista, sähköisistä, ohjelmallisista tapahtumista sekä lisäksi käyttötavoista ja käyttöympäristöstä johtuvat vaaratilanteet.
 - ii) Dokumentoituna mahdollisimman laaja listaus kaikista mahdollisista vaaratilanteista ja ne lähteet, joita on käytetty vaaroja tunnistettaessa
- c) Riskin suuruuden arviointi
 - i) Vaarat käydään läpi yksitellen, ja arvioidaan riskin merkitys vaaran todennäköisyyden ja seurauksen funktiona.
 - ii) Dokumentoidaan perustelut todennäköisyysarviolle

2) Riskin arviointi

- a) Riskin luokittelu
- b) Riskin suuruuden mukaan päätetään onko riski hyväksyttävä, voidaanko riski poistaa tai tuleeko riskiä pienentää

- c) Turvallisuusvaatimukset, mitkä tavoitteet on tarkoitus saavuttaa turvallisuustoimenpiteillä.
 - d) Dokumentoidaan mihin tietoihin riskin arviointi perustuu ja mitkä ovat valitut toimenpiteet
- 3) Riskin pienentäminen
- a) Luontaisesti turvalliset suunnittelutoimenpiteet
 - i) Hydraulikka
 - ii) Ohjausjärjestelmä
 - iii) Muut liikkuvan työkoneen järjestelmät
 - b) Suojaustoimenpiteet
 - i) Mekaaniset suojukset
 - ii) Sähköiset suojukset
 - c) Toiminnallinen turvallisuus
 - i) Turvallisuuteen liittyvät ohjausjärjestelmän osat
 - ii) Turvallisuusvaatimukset
 - iii) Suoritustasot
 - d) Tarkastetaan, ettei riskin pienentämisellä ole aiheutettu lisävaaraa muualle järjestelmään
- 4) Riskin pienentämisen todentaminen ja kelpuutus
- a) Turvallisuusvaatimusten täyttyminen
 - i) Mekaaninen, hydraulinen ja sähköinen järjestelmä
 - ii) Ohjausjärjestelmä
 - b) Testausmenetelmät
 - i) Testauspöytäkirjat
- 5) Jäännösriskit
- a) Ne liikkuvaan työkoneeseen jäävät riskit, jotka on huomioitava varoitustarroin käyttöoppaassa ja koulutuksessa.

Dokumenteissa tulee olla viittauksen niihin standardeihin, joiden mukaan eri työvaiheet ovat tehty.

Näiden dokumenttien ja asiakirjojen kautta koneen valmistaja voi osoittaa liikkuvan työkoneen vaatimustenmukaisuuden. Turvallisuussuunnittelu nähdään usein aikaa ja resursseja vievänä toimintana. Tämä on seurausta siitä, ettei koneasetuksen sisältöä tunneta, eikä vaatimuksia osata tuoda käytäntöön. Suurin osa riskianalyysistä ja riskien pienentämisen prosessista on osa laadukasta koneensuunnittelutyötä, ja suurin osa dokumenteista tulee tehdyksi normaalin suunnittelutyön ohessa. Jos liikkuvan työkoneen vaatimuksenmukaisuus joudutaan osoittamaan myöhemmin asiakkaan sitä vaatiessa, tai

tapaturman sattuessa, on dokumenttien kerääminen ja työkoneenturvallisuuden osoittaminen lähes mahdotonta.

Riskin arviointi ja riskianalyysi ovat liikkuvan työkoneen turvallisuuden kannalta keskeisiä työvaiheita. Jos vaaratilanteita ei ole tunnistettu, ei niiden pienentämiseksi ole toimenpiteitä. Riskin pienentämiseen käytetyt menetelmät, ja sen arviointi, milloin riski on tarpeeksi pieni, vaatii hyvää ammattitaitoa ja asiaan perehtymistä. Simulointia on 2000 -luvulla käytetty koneensuunnittelun apuna yhä enemmän. Reaaliaikaisen simuloinnin tuomat hyödyt turvallisuussuunnitteluun ovat merkittävät. HIL -simuloinnin avulla suunnittelutoimenpiteet voidaan kohdentaa sinne, missä niitä eniten tarvitaan.

LÄHTEET

- [1] Huhtala, K. Mobilehydrauliikka. 2013-2014. Hydrauliikan ja automatiikan laitos. Luentokalvot.
- [2] SFS-EN 62601. Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. Helsinki 2006, Suomen standardisoimisliitto. 197 s.
- [3] Airila, M. Mekatroniikka. 8. painos. Helsinki 2011, Otatieto. 389 s.
- [4] Kauranne, H., et al. Hydrauliteknikka 1. painos. Helsinki 2008, WSOY Oppimateriaali. 487 s.
- [5] Lehmusto, M. Hydraulijärjestelmän luotettavuus ja vikaantuminen. Espoo 1982, Valtion teknillinen tutkimuskeskus, Tiedotteita. 76 s.
- [6] Immonen, A. Hydraulikomponenttien käyttöään tarkastelu. Diplomityö. Tampere 2007, Tampereen teknillinen yliopisto, Konetekniikka. 85 s.
- [7] Backé, W., Jacobs, G. Contamination sensitivity of controlled variable displacement pumps and continuous valves. 44th Annual Earthmoving Industry Conference, Peoria, IL, United States, April 20-21, 1993. SAE Technical Paper 931177, 1993.
- [8] Tamminen, J. Mekaanisten ja hydraulisten komponenttien luotettavuudesta. Diplomityö. Tampere 1977, Tampereen teknillinen korkeakoulu. Konetekniikka. 104 s.
- [9] Järvenpää, J., Silvola, M. Hydrauliikan toiminnan turvallisuuden ja luotettavuuden parantaminen henkilönostolaitteilla. Helsinki 1992, Työsuojelurahasto. 90267.
- [10] Rinkinen, J., Koivula, T., Experiences and proposals for condition monitoring methods of hydraulic valves. Condition Monitoring and Diagnostics - International Seminar, September 28-29, 2005, Oulu, Finland.
- [11] Alatalo, M. et al. Metsäkoneiden hydrauliikan kunnossapidon työturvallisuus. Raportti n:o 37. Oulu 1983, Oulun yliopisto. Konetekniikan osasto. 83 s.

- [12] Rusanen, H., Koivula, T. & Rinkinen, J. 2005. Vika-, vaikutus- ja kriittisyys-analyysin laatiminen sekä hyödyntäminen. Teollisuushydrauliikan vianetsintä, Ramada Hotel Tampere, 6.-7.4.2005. Rajamäki, Kunnossapitoyhdistys. 8 s.
- [13] Hammaspyörä- ja mäntäpumput. FLUID Finland 03/2003: FLUID klinikka nro 5. S: 6–8.
- [14] Fonselius, J., Rinkinen, J., Vilenius, M. Hydrauliteknikka II, Tampere 2008, Tampereen Yliopistopaino Oy. 226 s.
- [15] SFS 2230. Hydrauliputkistot. Liitänäkierreet, tiivistetasot ja putket. Helsinki 1968. Suomen standardoimisliitto. 2 s.
- [16] Kiviniemi, A. Hydrauliletkujen luotettavuus. Diplomityö. Tampere 2000, Tampereen teknillinen korkeakoulu, Automaatiotekniikka. 80 s.
- [17] Kivistö-Rahnasto, J. 2009. Machine-related fatalities. Proceedings of the 17th World Congress on Ergonomics IEA 2009, CD-ROM. International Ergonomics Association. 4 p.
- [18] L 1016/2004. Laki eräiden teknisten laitteiden vaatimustenmukaisuudesta
- [19] Euroopan parlamentin ja neuvoston direktiivi 2006/42/EY. Konedirektiivi.
- [20] A 400/2008. Valtioneuvoston asetus koneiden turvallisuudesta.
- [21] Siirilä, T. Koneturvallisuus: EU:n direktiivien ja standardien soveltaminen käytännössä. 2. p. Espoo 2008, Inspecta. 462 s.
- [22] Euroopan komissio. Yritys ja teollisuustoiminta, CE-merkinä. [WWW]. [Vii-tattu 24.6.2014]. Saatavissa: http://ec.europa.eu/enterprise/policies/single-market-goods/cemarking/about-ce-marking/index_fi.htm
- [23] SFS-EN ISO 12100. Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. Helsinki 2010. Suomen standardoimisliitto. 171 s.
- [24] SFS-EN ISO 14121-1 Koneturvallisuus. Riskin arviointi. Osa 1: Periaatteet. Helsinki 2007. Suomen standardoimisliitto. 64 s.
- [25] SFS-ISO/TR 14121-2 Koneturvallisuus. Riskin arviointi. Osa 2: Käytännön opastusta ja esimerkkejä menetelmistä. Helsinki 2013. Suomen standardoimisliitto. 80 s.

- [26] Siirilä, T. Koneturvallisuus: EU-määräysten mukainen koneiden turvallisuus. 2. p. Espoo 2008, Inspecta. 431 s.
- [27] SFS-EN ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. Helsinki 2008. Suomen standardoimisliitto. 180 s.
- [28] Siirilä, T. Koneturvallisuus: Ohjausjärjestelmät ja turvalaitteet. 2. p. Espoo 2009, Inspecta. 472 s.
- [29] Hietikko, M., Malm, T. & Alanen, J. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. 2009, VTT Tiedotteita. 75 s.
- [30] SFS-EN ISO 13849-2 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus. Helsinki 2014. Suomen standardoimisliitto. 170 s.
- [31] SFS-EN ISO 13849-1 Koneturvallisuus. Sähköisten/elektronisten/ ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: Yleiset vaatimukset. Helsinki 2011. Suomen standardoimisliitto. 119 s.
- [32] SFS-EN ISO 4413. Hydraulinen tehonsiirto. Helsinki 2011. Suomen standardoimisliitto. 90 s.
- [33] Gauthier, F., Lambert, S. & Chinniah, Y. Experimental Analysis of 31 Risk Estimation Tools Applied to Safety of Machinery. International Journal of Occupational Safety and Ergonomics 18(2012)2, pp 245-265.
- [34] MacDonald, D. Practical machinery safety. Oxford 2004, Practical professional books from Elsevier. 289 s.
- [35] SFS-EN 61508-3. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 3: Ohjelmistovaatimukset. Helsinki 2011. Suomen standardoimisliitto. 202 s.
- [36] Lätti, M., Mäntälä, J. Pienkuormainten käytön toiminnallisuus ja työturvallisuus maatalousyrityksissä. Nurmijärvi 2007, TTS Tutkimuksen raportteja ja oppaita 32. 42 s.
- [37] Preventing Injuries and Deaths from Skid-Steer Loaders. National Institute for Occupational Safety and Health (NIOSH). 2011-128. 13 s. Saatavissa:

<http://www.cdc.gov/niosh/docs/2011-128/pdfs/2011-128.pdf>

- [38] Multanen, P., Saarinen, J., Hyvönen, M., Vilenius, M. Dynamic real-time simulation of intelligent mobile machines. 27th IASTED International Conference Modelling, Identification, and Control, February 11-13, 2008, Innsbruck, Austria.

LIITTEET**EY-vaatimustenmukaisuusvakuutus koneesta**
(Konedirektiivi 2006/42/EY, Liite II A)

Valmistaja: _____

Osoite: _____

Henkilön nimi, joka on valtuutettu kokoamaan teknisen tiedoston

Nimi: _____

Osoite: _____

Vakuuttaa että

- on konedirektiivin (2006/42/EY) asiaankuuluvien säännösten mukainen
- on seuraavien EY-direktiivien säännösten mukainen

ja lisäksi vakuuttaa, että

- seuraavia yhdenmukaistettuja standardeja on sovellettu

- seuraavia muita standardeja tai teknisiä eritelmiä on sovellettu

Paikka, aika _____

Allekirjoitus _____

Koneen tekninen tiedoston sisältö, koneasetus liite VII

1. Rakennetiedosto, jossa ovat

- koneen yleiskuvaus,
- koneen yleispiirustus ja siihen liittyvät ohjauspiirien piirustukset sekä asianmukaiset kuvaukset ja selitykset koneen toiminnan ymmärtämiseksi,
- täydelliset yksityiskohtaiset piirustukset laskelmineen, testaustuloksineen, todistuksineen ja muine tietoineen, joita tarvitaan tarkastettaessa, onko kone olennaisen terveys- ja turvallisuusvaatimusten mukainen,
- riskin arviointia koskevat asiakirjat, joista ilmenee noudatettu menettely, mukaan lukien
 - a. luettelo olennaisista terveys- ja turvallisuusvaatimuksista, jotka koskevat konetta,
 - b. niiden suojaustoimenpiteiden kuvaus, jotka on toteutettu tunnistettujen vaarojen poistamiseksi tai riskien pienentämiseksi ja tarvittaessa maininta koneeseen liittyvistä jäännösriskeistä,
- käytetyt standardit ja muut tekniset eritelvät siten, että käy ilmi, mitkä olennaiset terveys- ja turvallisuusvaatimukset kyseiset standardit kattavat,
- tekniset selosteet, joista ilmenevät niiden testien tulokset, jotka on tehnyt joko valmistaja tai valmistajan taikka tämän valtuutetun edustajan valitsema laitos,
- jäljennös koneen ohjeista,
- osittain valmiin koneen osalta tarpeen mukaan liittämismukautus ja osittain valmiin koneen asianmukaiset kokoonpano-ohjeet,
- tarpeen mukaan jäljennökset koneen tai muiden siihen liitettyjen tuotteiden EY-vaatimustenmukaisuusvakuutuksista,
- jäljennös EY-vaatimustenmukaisuusvakuutuksesta;

2. Sarjatuotteiden osalta ne sisäiset toimenpiteet, jotka pannaan täytäntöön sen varmistamiseksi, että kone pysyy tämän asetuksen tai sitä vastaavan direktiivin säännösten mukaisena.

Valmistajan on tehtävä komponenteille, tarvikkeille tai valmiille koneille tarpeelliset tutkimukset ja testit määrittääkseen, soveltuuko kone suunnittelunsa tai rakenteensa puolesta turvallisesti asennettavaksi ja käyttöön otettavaksi. Asiaankuuluvat selosteet ja tulokset on sisällytettävä tekniseen tiedostoon.